ifaci

institut français de l'audit et du contrôle internes

Cahier de la Recherche

Maîtriser le recours à des prestations externes d'audit

Cas de l'audit interne des systèmes d'information

Réalisé par une Unité de Recherche

L'IFACI est affilié à The Institute of Internal Auditors

Dans la même collection

- **La fraude interne dans les collectivités territoriales,** Groupe Professionnel « Collectivités territoriales » *(à paraître)*
- **Dispositifs de maîtrise des risques de fraude à l'assurance, à la retraite complémentaire et à l'action sociale,** Groupes Professionnels « Assurance » et « Protection Sociale » *(novembre 2015)*
- **L'audit des délégations de services publics,** Groupe Professionnel « Collectivités territoriales » *(mars 2015)*
- **Contrôle interne des opérateurs de l'Etat : Pour une maîtrise et un pilotage global des risques,** Unité de Recherche IFACI *(juin 2014)*
- **De la cartographie au plan d'audit,** Groupe Professionnel « Banque » *(décembre 2013)*
- **La cartographie des risques – 2ème édition,** Groupe Professionnel « Assurance » *(septembre 2013)*
- **L'audit du versement des subventions aux associations,** Groupe Professionnel « Collectivités Territoriales » *(février 2013)*
- **Sélectionner un outil informatique pour les services d'audit et de contrôle internes : un véritable projet,** Unité de Recherche Informatique IFACI *(décembre 2012)*
- **L'accès et la conservation des documents relatifs aux missions d'audit,** Unité de Recherche IFACI *(novembre 2012)*
- **La délégation de gestion en assurance de personnes : pistes pour un contrôle interne efficace,** Unité de Recherche IFACI *(juin 2012)*
- **Les variables culturelles du contrôle interne,** Unité de Recherche IFACI *(décembre 2011)*
- **Des clés pour la mise en œuvre et l'optimisation du contrôle interne,** Unité de Recherche IFACI *(octobre 2011)*
- **La fraude : Comment mettre en place un dispositif de lutte contre la fraude ?** Unité de Recherche de l'IFACI *(décembre 2010)*
- **La création de valeur par le contrôle interne,** Unité de Recherche de l'IFACI *(octobre 2010)*
- **Prise de Position du Groupe Professionnel Banque pour un urbanisme du contrôle interne efficient,** Groupe Professionnel « Banque » *(Avril 2010)*
- **L'audit de la fraude dans le secteur bancaire et financier,** Unité de Recherche de l'IFACI *(janvier 2010)*
- **Création et gestion d'une petite structure d'audit interne,** Unité de Recherche IFACI *(janvier 2009)*
- **Une démarche d'audit de plan de continuité d'activité,** Unité de Recherche IFACI *(juillet 2008)*
- **Guide d'audit du développement durable : comment auditer la stratégie et les pratiques de développement durable ?,** Unité de Recherche IFACI *(juin 2008)*
- **Contrôle interne et qualité : pour un management intégré de la performance,** Unité de Recherche IFACI *(mai 2008)*
- **Evaluer et développer les compétences des collaborateurs,** Antenne régionale Aquitaine IFACI *(novembre 2007)*
- **Audit des prestations essentielles externalisées par les établissements de crédit et les entreprises d'investissement– 2ème Edition,** Groupe Professionnel « Banque » *(janvier 2007)*
- **La cartographie des risques,** Groupe Professionnel « Assurance » *(juillet 2006)*
- **L'audit interne et le management des collectivités territoriales,** Unité de Recherche IFACI *(mai 2006)*
- **Une démarche de management des connaissances dans une direction d'audit interne,** Unité de Recherche IFACI *(mai 2006)*
- **L'auto-évaluation du contrôle interne,** Unité de Recherche IFACI *(octobre 2005)*
- **Cartographie des Risques,** Groupe Professionnel « Immobilier Locatif » *(septembre 2005)*
- **Étude du processus de management et de cartographie des risques,** Groupe Professionnel « Industrie et commerce » *(janvier 2004)*
- **Pour un bon audit du dispositif de lutte contre le blanchiment des capitaux,** Groupe Professionnel « Banque » *(février 2004)*
- **L'efficacité des Comités d'audit – Les meilleures pratiques,** PwC – The IIA Research Foundation – Traduction IFACI – PwC *(mai 2002)*
- **Gouvernement d'entreprise et Conseil d'administration,** PwC – The IIA Research Foundation – Traduction IFACI – PwC *(mai 2002)*
- **Évaluation de la compétence dans la pratique de l'audit interne,** Prise de position de l'ECIIA – Traduction IFACI *(2001)*
- **Management des risques,** IIA UK – Traduction Unité de Recherche IFACI *(2001)*
- **Le rôle de l'auditeur interne dans la prévention de la fraude,** Prise de position de l'ECIIA – Traduction IFACI *(2000)*

Pour plus d'informations : www.ifaci.com

© IFACI – Paris – novembre 2015

ISBN : 978-2-915042-73-3 – ISSN : 1778-7327

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

Remerciements

L'IFACI tient tout particulièrement à remercier toutes les personnes qui ont contribué aux différentes étapes de l'élaboration de ce cahier dans le cadre l'unité de recherche animée par **Philippe HERVIAS,** *Directeur Audit SI, Audit Interne Groupe, SANOFI, Vice-Président du Groupe Professionnel « Systèmes d'Information » de l'IFACI.*

- Rédaction :

  Lionel ARBEY, *Chef de mission Inspection Générale, La Banque Postale*

  Béatrice KI-ZERBO, *Directeur de la Recherche, IFACI*

  Guillaume LAMY, *Auditeur, adjoint au chef de la mission ministérielle d'audit interne, Conseil général de l'environnement et du développement durable, Ministère de l'Écologie, du Développement Durable et de l'Énergie*

  Yohann VERMEREN, *Associé, KPMG*

- Autres contributeurs :

  Romain CAMUS, *Associé, PwC*

  Philippe LARDY, *Chef de mission audit interne, EDF*

  Olivier SZNITKIES, *Audit Director, LafargeHolcim*

- Réviseurs :

  José BOUANICHE, *Auditeur interne, CAISSE DES DEPÔTS, Président du Groupe Professionnel « Systèmes d'Information » de l'IFACI*

  Xavier ORTMANS, *Directeur de l'audit et du pilotage stratégique, Etablissement Français du Sang*

  Corinne LABIELLE, *Directeur de l'audit interne, LA MUTUELLE GENERALE*

- Suivi et mise en forme :

  Bouchra BAJJOU, *Chef de projets recherche, IFACI*

L'IFACI, remercie également les responsables de contrôle interne et d'audit interne qui ont participé au *benchmark* et à l'atelier organisés en avril 2015.

Philippe MOCQUARD, *Délégué Général, IFACI*

© IFACI

Sommaire

REMERCIEMENTS 3

INTRODUCTION 7

1- UNIVERS ET ENJEUX DES PRESTATIONS EXTERNES D'AUDIT DES SI 11
1.1- Une typologie de missions d'audit des SI 12
1.1.1- Audit de la gouvernance des SI 13
1.1.1.1- Audit du pilotage des infrastructures informatiques 14
1.1.1.2- Audit des prestations informatiques externalisées 14
1.1.2- Support à la revue de processus opérationnels et fonctionnels 15
1.1.2.1- Revue de l'informatique décisionnelle et du contrôle en continu 15
1.1.2.2- Contrôles applicatifs 16
1.1.2.3- Les audits de conformité ou de régularité 17
1.1.3- Contrôles généraux informatiques (relatifs à des applications ou à des infrastructures SI) 17
1.1.3.1- Les audits de projets (développement, maintenance et changements) 18
1.1.3.2- Audit de la sécurité SI 18
1.1.3.3- Contrôles des accès physiques et logiques 19
1.1.3.4- Audit de la production informatique 20
1.1.3.5- Audit du support utilisateurs 20
1.1.3.6- Audit du plan de secours 21
1.2- Avantages et inconvénients du recours à des prestations externes 22
1.2.1- Typologie des prestations externes d'audit 22
1.2.2- Motifs classiques de recours à des prestations externes 23
1.2.3- Facteurs limitants et inconvénients 23

2- ORIENTATIONS CONCERNANT LE RECOURS A DES PRESTATIONS EXTERNES 25
2.1- Stratégie de gestion des ressources du service d'audit 26
2.1.1- Détermination d'un modèle de gestion des compétences 26
2.1.2- Définition d'une politique de recours à des prestations externes 26
2.1.2.1- Interagir avec les instances de gouvernance 27
2.1.2.2- Maîtriser les opportunités et les risques 28
2.1.2.3- Prendre en compte le contexte réglementaire et technique 29
2.1.2.4- Couvrir l'univers d'audit 30
2.1.3- Déclinaison opérationnelle de la politique 31
2.2- Orientations pour la gestion des prestations externes au niveau d'une mission 31
2.2.1- Spécifications de la mission 31
2.2.1.1- Constitution de l'équipe 32
2.2.1.2- Méthodes et outils requis 36
2.2.2- Prise de décision 36

© IFACI

3- MODALITES PRATIQUES D'ENGAGEMENT D'UN PRESTATAIRE 39
3.1- Mise en concurrence et sélection du prestataire 40
3.1.1- Mise en concurrence : les points essentiels de l'appel d'offres 40
3.1.1.1- Principes généraux de recours à des services intellectuels 40
3.1.1.2- Modalités opérationnelles de réalisation de l'appel d'offres 40
3.1.2- La sélection du prestataire 43
3.1.2.1- Impact de la nature et du contexte de la mission 43
3.1.2.2- Evaluation des offres 43
3.2- Contractualisation 47
3.2.1- Eléments à prendre en considération 48
3.2.2- Clauses spécifiques 50

4- PILOTAGE DE LA PRESTATION ET DE LA MISSION 51
4.1- Cadre de pilotage à mettre en œuvre 52
4.2- Gestion de la relation avec le prestataire 54
4.2.1- Contrôle des profils 54
4.2.2- Gestion de l'équipe de prestataires et de l'environnement de travail 55
4.2.3- Maîtrise des interactions entre le prestataire et les audités 56
4.3- Contrôle des travaux réalisés 57
4.3.1- Maîtrise de la méthodologie 57
4.3.2- Maîtrise et déploiement des outils 58
4.3.3- Contrôles des analyses et des conclusions du prestataire 58
4.4- Contrôle de l'efficience du contrat et plans d'actions 60

ANNEXES 63
Annexe 1 : Exemple de missions d'audit des SI 64
Annexe 2 : Tableau de suivi 68
Annexe 3 : Exemple de grille d'évaluation de fin de mission à adapter en fonction du type de prestation (co-traitance ou pas) 76

BIBLIOGRAPHIE 78

Avertissement aux lecteurs

Ce cahier de la recherche a été réalisé à partir de contributions de professionnels de l'audit et du contrôle internes. Ce travail collectif, réalisé sous l'égide de l'IFACI, fournit un état des lieux des pratiques professionnelles et des pistes d'amélioration qui n'engagent pas les établissements et administrations représentés.

© IFACI

© IFACI

INTRODUCTION

© IFACI

Comme tout manager, le responsable de l'audit interne (RAI) s'organise, gère des moyens, pour atteindre ses objectifs qui s'inscrivent dans l'univers d'audit et le plan d'audit annuel à couvrir. Il lui faut également tenir compte des demandes des métiers en recherchant l'équilibre optimal de ressources toujours plus rares surtout dans des domaines d'expertise tels que les systèmes d'information (SI).

Pour faire face à ces responsabilités, et en fonction de ses choix stratégiques, le RAI peut décider de s'appuyer sur des équipes internes ou de faire appel ponctuellement ou de manière récurrente à des prestations externes. Le RAI doit alors mettre en place des dispositifs de maîtrise de ces prestations car sa responsabilité ne s'externalise pas. Il devra en particulier s'assurer du niveau de couverture des risques[1] et être convaincu de l'opinion du prestataire. Quel que soit le prestataire, le RAI devra s'assurer d'une prestation professionnelle notamment au regard des Normes d'audit interne (cf. Prise de position[2], Norme 2070[3], MPA 2120-2[4]).

Avec ce cahier de la Recherche, l'IFACI souhaite accompagner les RAI dans l'élaboration de leur stratégie de gestion des ressources et la maîtrise des éventuelles prestations externes.

Le comité de pilotage de la Recherche de l'IFACI a soutenu cette initiative du groupe professionnel SI compte tenu :

- du taux important de dispositifs de contrôle interne clés susceptibles de reposer sur un système informatisé (cf. GTAG « Management de l'audit des systèmes d'information »[5]) ;
- de l'impact des SI sur le niveau de maîtrise des risques stratégiques et opérationnels d'une organisation ;
- de la complexité de l'univers d'audit des SI ;
- des pratiques de recours à des prestataires dans ce domaine, que le service d'audit interne (SAI) dispose ou non d'auditeurs informatiques.

Véritable guide d'accompagnement, ce cahier de la Recherche est structuré autour des axes suivants :

- Univers et enjeux
- Orientations concernant le recours à des prestations externes
- Modalités pratiques d'engagement d'un prestataire
- Pilotage de la prestation et de la mission

---

[1] *Pour les risques SI voire : A global look at IT audit best practices - ISACA / PROTIVITI, 2014*

[2] *Prise de position de l'IIA sur les ressources de l'audit interne, Janvier 2009*

[3] *Cadre de Référence International des Pratiques Professionnelles (CRIPP 2014) : Norme 2070 « Responsabilité de l'organisation en cas de recours à un prestataire externe pour ses activités d'audit interne » - IIA / IFACI*

[4] *CRIPP 2014 : Modalité Pratique d'Application 2120-2 «Gestion du risque lié à l'activité d'audit interne » - IIA / IFACI. Ces lignes directrices étant régulièrement mises à jour, veuillez consulter le site de l'IFACI : www.ifaci.com*

[5] *Global Technology Audit Guide (GTAG) 4 : Management de l'audit des systèmes d'information, (2ème édition) - IIA / IFACI, 2013*

© IFACI

Ce cadre de pilotage des prestations externes d'audit des SI comporte des aspects génériques que l'unité de recherche a choisi d'intégrer pour permettre à tout service d'audit d'enrichir son dispositif et de maîtriser ces prestations de bout en bout. Par ailleurs, ce cadre étendu pourra être aisément appliqué pour le suivi de missions concernant d'autres domaines d'expertise (finance, actuariat, trading, ingénierie, fiscalité, droit ...).

Ce cahier ne traite pas des prestations réalisées par des départements de l'organisation à la demande de l'audit interne ni des prestations externes non mandatées par le service d'audit interne (prestations pour le compte de la DSI ou de la direction générale). Néanmoins, les bonnes pratiques proposées pourront être transposées à ce type de prestations.

© IFACI

© IFACI

Partie 1

Univers et enjeux des prestations externes d'audit des SI

Le responsable de l'audit interne peut décider de recourir à des prestations externes (cf. 2- Orientations concernant le recours à des prestations externes) pour une meilleure couverture des domaines SI de l'univers d'audit. Le choix d'une prestation dépend du type de mission à réaliser (cf. 1.1- Une typologie de missions d'audit des SI) et s'appuie sur l'analyse de l'opportunité et des contraintes du recours à des ressources externes (cf. 1.2- Avantages et inconvénients du recours à des prestations externes).

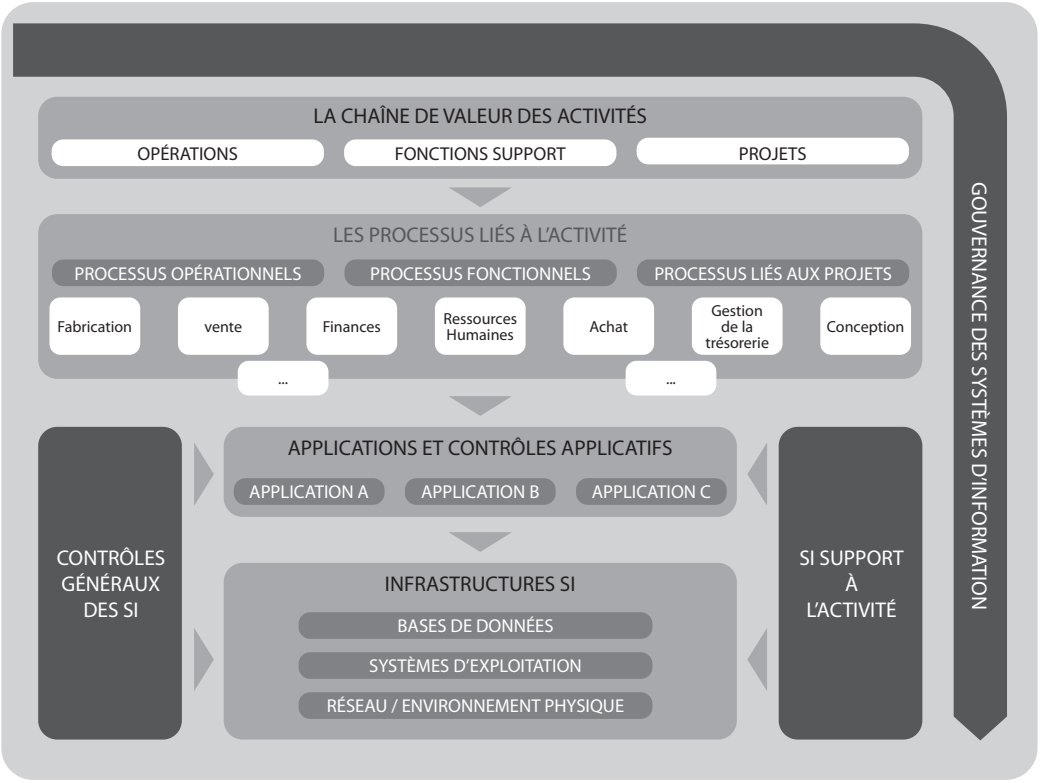
© IFACI

1.1- Une typologie de missions d'audit des SI

Le SI supporte la chaîne de valeur d'une organisation. Au-delà des aspects techniques, la maîtrise du SI passe par la prise en compte des aspects organisationnels. Cette double dimension et l'omniprésence des SI donnent de la complexité à l'univers d'audit des SI.
En outre, dans la pratique, cet univers ne peut pas être appréhendé de manière dissociée du reste du périmètre d'intervention de l'audit interne. Pour les besoins du présent cahier et en nous appuyant sur le GTAG relatif à l'élaboration du plan d'audit des SI, nous cartographions cet univers autour de trois grands thèmes :

- Gouvernance des SI
- Support aux processus liés à l'activité
- Contrôles généraux des SI

Schéma n°1 : Cartographie de l'univers d'audit des SI



Adapté à partir du GTAG : Élaboration d'un plan d'audit des SI. Figure 3. Prendre en compte l'environnement du SI de l'organisation.p.6 - IIA/IFACI, 2008[6]

[6] *Global Technology Audit Guide (GTAG) 11 : Élaboration d'un plan d'audit des SI - IIA/IFACI, 2013*

© IFACI

L'annexe 1 propose des exemples de missions pour chacune de ces catégories. Vous trouverez ci-dessous une ébauche d'objectifs d'audit qui sont à prendre comme des points d'entrée pour mieux appréhender les enjeux de ces missions dans votre propre contexte et évaluer votre niveau de couverture actuel ou à moyen terme.

1.1.1- Audit de la gouvernance des SI

Enjeux : Dans leur relation au fait informatique, les organisations sont amenées à définir leurs priorités, leurs besoins fonctionnels et qualitatifs (ergonomie, performance, niveau de service…), les modalités d'allocation de leurs ressources humaines et financières, ainsi que les processus leur permettant de disposer d'une informatique en phase avec ces besoins (alignement fonctionnel), réactive, sûre et efficiente.

Objectifs d'audit : Pour évaluer la « maturité » de l'organisation dans ce domaine, l'auditeur peut porter une appréciation sur la capacité de l'organisation à piloter et utiliser son SI, à apprécier ses enjeux (notamment la valeur de son patrimoine numérique) et à évaluer les risques associés. Il peut aussi évaluer l'alignement du SI sur les objectifs stratégiques de l'organisation ou encore l'adéquation du rôle, du positionnement et des objectifs de la fonction SI avec les enjeux de l'organisation. Les missions d'audit pouvant être rattachées au thème de la gouvernance sont très variées. Certaines sont citées dans l'annexe 1 ou dans les références ci-dessous.

Pour en savoir plus

- Global Technology Audit Guide (GTAG®) 1 « Le contrôle et le risque des systèmes d'information » / IIA / IFACI, 2ème édition, mars 2013
- Global Technology Audit Guide (GTAG®) 4 « Management de l'audit des systèmes d'information » / IIA / IFACI, 2ème édition, mars 2013
- Global Technology Audit Guide (GTAG®) 17 « Auditing IT Governance »» / IIA, juillet 2012
- COBIT 5.0 « Un référentiel orienté affaires pour la gouvernance et la gestion des TI de l'entreprise » / ISACA, 2012
- ITIL® 2011 (Information Technology Infrastructure Library) « Stratégie des services » / OGC (l'office de commerce britannique)
- Global Technology Audit Guide (GTAG®) 12 « Audit des projets des SI » / IIA / IFACI, mars 2009
- Global Technology Audit Guide (GTAG®) 11 « Elaborer le plan d'audit des SI » / IIA / IFACI, juillet 2008
- Cloud computing et protection des données / AFAI / IFACI / CIGREF, mars 2013

© IFACI

1.1.1.1- Audit du pilotage des infrastructures informatiques

Enjeux : Avec l'importance croissante des systèmes d'information au sein des organisations, le pilotage des infrastructures informatiques (bases de données, systèmes d'exploitation, réseaux, environnement matériel et physique) revêt un enjeu majeur notamment en termes de disponibilité, de performance et de capacité.

Objectifs d'audit : Les missions d'audit des infrastructures informatiques vont permettre de s'assurer de l'efficacité, de la continuité et de l'alignement stratégique du SI. Par exemple, l'évaluation des modalités et moyens mis en œuvre (schémas d'organisation, rôles et responsabilités, architecture, politiques, suivi budgétaire, indicateurs de pilotage).
Ces missions peuvent s'accompagner d'une revue des contrôles généraux liés aux éléments d'infrastructure audités (cf. 1.1.3).

Pour en savoir plus

- ITIL® 2011 (Information Technology Infrastructure Library) « Exploitation des services / OGC (l'office de commerce britannique)

1.1.1.2- Audit des prestations informatiques externalisées

Enjeux : Pour des questions de flexibilité ou de recentrage sur leur cœur de métier, il n'est pas rare que les organisations fassent appel à de l'externalisation aussi diverse que l'infogérance, la tierce maintenance applicative, l'assistance technique ou la fourniture de service d'application hébergée (dont le cloud).
Même pour les activités métiers externalisées, les organisations restent tenues de maîtriser le système d'information sous-jacent.

Objectifs d'audit : L'auditeur peut intervenir à toutes les phases d'une prestation informatique externalisée, de la spécification des besoins au bilan de mise en œuvre et prendre en compte l'évaluation de la gestion du niveau de service.
L'auditeur pourra apporter une valeur ajoutée en analysant la rentabilité de la stratégie d'externalisation, la gestion RH sous-jacente (dont le risque d'homme-clé), la gestion de la connaissance, le pilotage contractuel et opérationnel des prestations, la réversibilité de la prestation, l'atteinte des niveaux et de la qualité de service attendu.
Dans le cadre d'activités métiers externalisées, l'audit devra a minima s'assurer du respect des engagements contractuels, des modalités d'échanges de données et autres problématiques informatiques en lien avec l'atteinte des objectifs de l'organisation .

© IFACI

Pour en savoir plus

- eSourcing Capability Model pour les organisations clientes (eSCM-CL) / Bill Hefley, Ethel Loesche. Translated by Eric Baussand and Eric Herr, mai 2014
- Cloud computing et protection des données / AFAI / IFACI / CIGREF, mars 2013
- Global Technology Audit Guide (GTAG®) 7 « L'infogérance » / IIA / IFACI, 2ème édition, juin 2012
- Gouvernance du système d'information / CIGREF / IFACI, octobre 2011
- ITIL® 2011 (Information Technology Infrastructure Library) « Conception des services » / OGC (l'office de commerce britannique)
- Outsourced IT Environments Audit/Assurance Program / ISACA, 2009

1.1.2- Support à la revue de processus opérationnels et fonctionnels

Enjeux : Un processus est une succession d'activités indissociables des personnes et des outils qui permettent de les réaliser. L'évaluation de l'efficacité d'un processus nécessite donc l'examen des systèmes informatiques qui en soutiennent l'exécution.

Objectifs d'audit : L'audit devra apprécier l'adéquation du SI (efficacité, efficience, sécurité, résilience) aux objectifs du processus audité et sa contribution au dispositif de contrôle interne. Les missions d'audit pourront porter sur la conformité de mise en œuvre par rapport à l'objectif du traitement, l'examen de la qualité des données en entrée, au cours et en sortie du processus (cf. 1.1.2.1), ainsi que la maîtrise de la chaîne de traitement y compris les interfaces avec d'autres processus. L'audit pourra également s'assurer de l'efficacité des applications qui automatisent tout ou partie des tâches ou procédures qui le composent.

Pour en savoir plus

- Le contrôle interne du système d'information des organisations / IFACI / CIGREF, février 2009
- Global Technology Audit Guide (GTAG®) 8 « Audit des contrôles applicatifs » / IIA / IFACI, juillet 2007

1.1.2.1- Revue de l'informatique décisionnelle et du contrôle en continu

Enjeux : L'informatique décisionnelle permet de collecter, consolider et restituer les données d'une organisation. Elle donne aux décideurs et aux opérationnels une vue d'ensemble de l'activité traitée. Pour soutenir une prise de décision efficace, une réduction des coûts de contrôle et l'amélioration de la lisibilité des opérations, la qualité[7] et l'analyse des données sont cruciales.

[7] *Selon le COSO (cf. pp171-172 du Référentiel de contrôle interne. Principes de mise en œuvre et de pilotage / Eyrolles 2014), la qualité des informations suppose que celles-ci soient accessibles, exactes, à jour, protégées, conservées, suffisantes, disponibles en temps voulu, valides et vérifiables.*

© IFACI

Par ailleurs, le contrôle en continu, processus exécuté par le management pour vérifier en permanence si les dispositifs de contrôle interne fonctionnent efficacement[8], s'appuie, entres autres, sur l'informatique décisionnelle.
L'efficacité du contrôle en continu dépend de la qualité des données et des traitements réalisés.

Objectifs d'audit : En fonction du niveau de maturité (de l'analyse ponctuelle de données au contrôle en continu) des organisations, les missions d'audit pourront examiner la qualité des données, l'adéquation des requêtes conçues et mises en œuvre par les opérationnels, ainsi que la pertinence des analyses au regard des objectifs de l'organisation. Ces missions pourront également évaluer la mise en œuvre des plans d'action résultant de ces analyses ainsi que les éventuels mécanismes de contrôle en continu mis en place par les opérationnels.
En l'absence d'un contrôle en continu robuste, le responsable de l'audit interne peut envisager des missions s'appuyant sur des techniques d'audit en continu.

Pour en savoir plus

- Global Technology Audit Guide (GTAG®) 3 « Audit continu : Coordonner l'audit et le contrôle en continu pour fournir une assurance continue» / IIA / IFACI, 2ème édition, mai 2015
- Cadre de Référence International des Pratiques Professionnelles de l'Audit Interne « MPA 2320-4 » / IIA / IFACI, septembre 2014
- ITIL® 2011 (Information Technology Infrastructure Library) « Conception des services » / OGC (l'office de commerce britannique)
- Monitoring Internal Control Systems and IT / ISACA, 2010

1.1.2.2- Contrôles applicatifs

Enjeux : Les applications informatiques, qui accompagnent, automatisent, ou se substituent à tout ou partie d'un processus métier, doivent assurer des niveaux de fiabilité, de performance et de sécurité adéquats.
Les contrôles applicatifs incluent, par exemple, les éditions de données, la conformité de séparation des fonctions, la balance des totaux de contrôle, la journalisation des transactions et les rapports d'erreurs.

Objectifs d'audit : L'audit des contrôles applicatifs[9] pourra évaluer que :

- les données d'entrée sont exactes (notion d'image fidèle), complètes, autorisées et correctes ;
- les données sont traitées conformément aux objectifs et dans un délai acceptable ;
- les données stockées et de sortie sont exactes et complètes ;

[8] *Global Technology Audit Guide (GTAG) 3 « Audit continu : Coordonner l'audit et le contrôle en continu pour fournir une assurance continue» / IIA / IFACI, 2ème édition, mai 2015*

[9] *Global Technology Audit Guide (GTAG) 8 « Audit des contrôles applicatifs » / IIA / IFACI, juillet 2007*

© IFACI

- une traçabilité du processus est assurée (piste d'audit) ;
- la séparation des fonctions est mise en œuvre par une gestion des droits d'accès, des rôles et profils utilisateurs appropriée.

Ce type de mission peut intégrer une revue des paramètres, une revue de code, voire la mise en œuvre de jeux d'essai qui permettront de mesurer l'exactitude et la complétude des données de sortie ainsi que le temps nécessaire à leur traitement.

Pour en savoir plus

- ITIL® 2011 (Information Technology Infrastructure Library) « Exploitation des services » / OGC (l'office de commerce britannique)
- Le contrôle interne du système d'information des organisations / IFACI / CIGREF, février 2009
- Generic Application Audit / Assurance Program / ISACA, 2009
- Guide d'audit des applications informatiques / ISACA / AFAI, 2008
- Global Technology Audit Guide (GTAG®) 8 « Audit des contrôles applicatifs » / IIA / IFACI, juillet 2007

1.1.2.3- Les audits de conformité ou de régularité

Enjeux : La réglementation externe, voire les instructions internes, imposent des contraintes susceptibles d'impacter le système d'information.

Objectifs d'audit : L'auditeur cherche dans ce cas à vérifier la conformité des contrôles automatisés aux référentiels normatifs et réglementaires qui s'imposent aux processus de l'organisation auditée. Il évalue également la complémentarité avec les contrôles manuels. Ceci implique mais ne se limite pas à l'audit des ressources informatiques supportant ces processus.
L'audit de conformité peut aller jusqu'à porter une appréciation sur la valeur de la contribution de l'informatique à la régularité des opérations auditées.

Pour en savoir plus

- Cahier de la recherche - L'audit des délégations de service public / Groupe Professionnel « Collectivités territoriales », mars 2015
- Global Technology Audit Guide (GTAG®) 13 « Fraud prevention and detection in an automated world » / IIA, décembre 2009
- Cahier de la recherche - Audit des prestations essentielles externalisées par les établissements de crédit et les entreprises d'investissement / Groupe Professionnel « Banque », janvier 2007

© IFACI

1.1.3- Contrôles généraux informatiques (relatifs à des applications ou à des infrastructures SI)

Les contrôles généraux informatiques sont déterminants pour l'efficacité et la fiabilité des SI. Ils incluent le développement, la maintenance, la gestion des changements, le support aux utilisateurs, le contrôle des accès physiques et logiques, la sécurité SI, la production et le plan de secours. Les contrôles généraux sont revus par l'audit interne car ils sont la base de l'environnement de contrôle des SI.
Si certaines missions très précises et très pointues nécessitent une expertise informatique, l'auditeur interne non spécialiste en SI pourra aborder les domaines identifiés ci-après :

1.1.3.1- Les audits de projets (développement, maintenance et changements)

Enjeux : La plupart des projets métiers contiennent une dimension informatique. Par ailleurs, la direction des systèmes d'information (DSI) initie des projets de maintenance ou de renouvellement qui peuvent impacter les métiers. L'anticipation des spécifications et l'adéquation des solutions informatiques est clé pour la réussite des projets et la performance des métiers.

Objectifs d'audit : L'auditeur peut intervenir à toute phase du projet (étude d'opportunité, conduite du projet, revue post-déploiement, revue de l'appropriation par les utilisateurs).
L'audit d'un projet pourra s'assurer de :

- la prise en compte des enjeux métiers (notion d'alignement) ;
- la qualité du pilotage ;
- la pertinence des spécifications ;
- l'adéquation des moyens humains, financiers et matériels, ainsi que des délais au regard des enjeux ;
- la conformité des programmes et des traitements aux spécifications ;
- l'opérationnalité des solutions SI (environnement de programmation, modèle de données, tests, mise en œuvre et déploiement) ;
- la maîtrise de la conduite du changement ;
- la réalisation d'objectifs prédéfinis et mesurables et de la robustesse des éventuels plans de maîtrise.

Pour en savoir plus

- Build, acquire & implement - BAI01 Manage programmes & projects Audit / assurance program / ISACA, 2014
- ITIL® 2011 (Information Technology Infrastructure Library) « Stratégie des services », « Transition des services », « Amélioration continue des services » / OGC (l'office de commerce britannique)
- Global Technology Audit Guide (GTAG®) 12 « Audit des projets SI » / IIA / IFACI, mars 2009

© IFACI

- Le contrôle interne du système d'information des organisations / IFACI / CIGREF, février 2009
- Change Management Audit / Assurance Program / ISACA, 2009

1.1.3.2- Audit de la sécurité SI

Enjeux : Protéger l'organisation contre le risque d'indisponibilité du SI, d'accès non autorisés (notamment liés à des intrusions), de perte, d'altération ou de divulgation d'informations qui constituent un actif précieux.

Objectifs d'audit : La sécurité est une démarche globale de l'organisation organisée autour d'une politique de sécurité SI.
La mission d'audit pourra évaluer :

- l'existence et la pertinence de la politique de sécurité SI au regard de la stratégie et des besoins de l'organisation ;
- la gouvernance de la sécurité des SI (rôles et responsabilités du conseil d'administration, de la direction générale, de la DSI, du management opérationnel) ;
- l'efficacité des tests de sécurité et la pertinence des indicateurs ;
- les canaux de reporting et les suites données aux constats de vulnérabilité ;
- l'efficience des systèmes de sécurité (l'adéquation des moyens de détection et de protection avec les enjeux métier et la valeur de l'information) ;
- la gestion de crise en cas d'incident de sécurité.

Pour en savoir plus

- Le rôle de l'audit interne face aux cyberisques / IIARF / IFACI, 2015
- ITIL® 2011 (Information Technology Infrastructure Library) « Conception des services » / OGC (l'office de commerce britannique)
- Global Technology Audit Guide (GTAG®) 15 « Information Security Governance » / IIA, Juin 2010

1.1.3.3- Contrôles des accès physiques et logiques

Enjeux : La surveillance et le contrôle des accès aux bâtiments ou aux systèmes sont indispensables pour protéger les actifs matériels et immatériels des organisations.

Objectifs d'audit : Une mission d'audit des accès physiques et logiques permet d'évaluer la pertinence et l'efficacité des dispositifs permettant de sécuriser ces accès. Il s'agira notamment de passer en revue :

© IFACI

- la formalisation et l'efficacité du processus de gestion des accès (identification et authentification des utilisateurs, attribution des droits d'accès, gestion des privilèges, procédures dérogatoires…) en fonction des choix de séparation des fonctions, des niveaux d'autorisation et du « besoin d'en connaître » ;
- la traçabilité de l'activité des utilisateurs et des informaticiens (notamment des comptes à privilèges) ;
- la détection et le traitement des accès non autorisés aux ressources informatiques.

Pour en savoir plus

- ITIL® 2011 (Information Technology Infrastructure Library) « Exploitation des services » / OGC (l'office de commerce britannique)
- Le contrôle interne du système d'information des organisations / IFACI / CIGREF, février 2009
- Global Technology Audit Guide (GTAG®) 9 « Gestion des identités et des accès » / IIA / IFACI, novembre 2007

1.1.3.4- Audit de la production informatique

Enjeux : Pour assurer la permanence et la continuité de leurs opérations SI, les organisations se doivent d'évaluer les moyens humains et techniques, ainsi que les processus mis en œuvre par la fonction informatique, pour suivre le déroulement de ses opérations et en assurer la disponibilité en lien avec les niveaux de service (SLA-Service Level Agreement) définis avec les propriétaires de processus.

Objectifs d'audit : Il s'agit dans ce type d'audit d'analyser l'adéquation des moyens humains, matériels, logiciels et organisationnels (procédures d'exploitation, de sauvegarde, de restauration, de gestion de la capacité, de gestion des configurations et des incidents …) mis en œuvre pour répondre aux enjeux de l'organisation. Ces missions permettent de vérifier la maîtrise opérationnelle des éléments constituants le système d'information, y compris son infrastructure (serveurs, commutateurs, routeurs, baies de stockage, technologies de virtualisation…).

Pour en savoir plus

- ITIL® 2011 (Information Technology Infrastructure Library) « Transition des services » / OGC (l'office de commerce britannique)

1.1.3.5- Audit du support utilisateurs

Enjeux : Améliorer en permanence le niveau d'appropriation du SI par les utilisateurs et la performance globale des systèmes (compréhension des besoins des utilisateurs, qualité de la gestion des incidents, disponibilité, temps d'accès…).

© IFACI

Objectifs d'audit : La mission d'audit vérifiera que la fonction de support prend en compte les besoins des métiers pour y répondre de manière adaptée, dispose d'un niveau de ressources approprié et contribue à la mise en œuvre de procédures (enregistrement et documentation des incidents, analyse d'impact, classification et priorisation, traitement ou escalade vers des spécialistes, suivi et communication de la résolution, gestion des changements).

Pour en savoir plus

- ITIL® 2011 (Information Technology Infrastructure Library) « Transition des services », « Amélioration continue des services » / OGC (l'office de commerce britannique)

1.1.3.6- Audit du plan de secours

Enjeux : Concourir à la continuité des activités métiers par la définition d'une stratégie et la mise en place de solutions de rétablissement des SI après incident. Cette restauration des SI passe par la reprise testée des données, des systèmes et des procédures associées ainsi que les moyens humains nécessaires au niveau des métiers et de la DSI.

Objectifs d'audit : L'audit interne pourra fournir une assurance quant à :

- La bonne intégration au plan de continuité d'activité de l'organisation
- la pertinence de la documentation du plan de secours au regard des besoins de continuité des métiers (analyse d'impacts ou BIA-Business Impact Analysis, niveaux de service ou SLA-Service Level Agreement)
- la répartition des responsabilités définies dans le plan de secours
- la documentation des solutions de secours préconisées (instructions détaillées du plan, le renvoi aux procédures de production, les diagrammes présentant les systèmes…)
- l'efficacité de tests conduits périodiquement et la capacité de reprise après sinistre
- l'actualisation des procédures de reprise lorsque les processus et les systèmes de l'organisation évoluent

Pour en savoir plus

- Practice Guide « Business Continuity Management » / IIA, Août 2014
- ITIL® 2011 (Information Technology Infrastructure Library) « Conception des services » / OGC (l'office de commerce britannique)
- Business Continuity Management Audit / Assurance Program / ISACA, 2011
- Global Technology Audit Guide (GTAG®) 10 « Gestion de la continuité d'activité » / IIA / IFACI, juillet 2008

© IFACI

1.2- Avantages et inconvénients du recours à des prestations externes

1.2.1- Typologie des prestations externes d'audit

Les prestations externes sont caractérisées[10] selon :

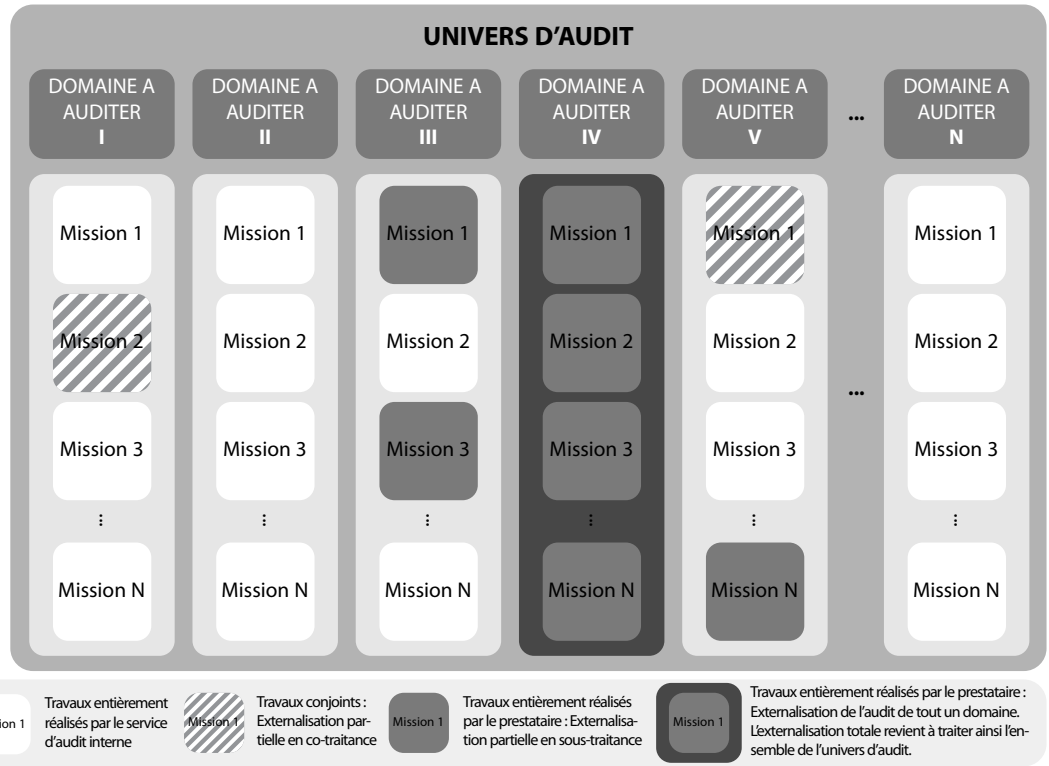
- la part des missions du plan d'audit interne déléguées à des prestataires extérieurs ;
- la présence ou non de travaux conjoints entre intervenants extérieurs et audit interne ;

Le tableau ci-après recense différentes pratiques d'externalisation.

Part de missions déléguées	Travaux conjoints	Travaux entièrement réalisés par le prestataire
100 %	N / A	Externalisation totale
Moins de 100 %	Externalisation partielle en co-traitance	Externalisation partielle en sous-traitance
0 %	Absence d'externalisation	

Selon la stratégie une ou plusieurs de ces pratiques d'externalisation pourront être utilisées pour couvrir l'univers d'audit.

Schéma n°2 : Représentation de l'univers d'audit selon le type de prestations



[10] *Prise de position de l'IIA sur les ressources de l'audit interne, p.5. IIA, Janvier 2009*

© IFACI

Pour mémoire

Norme 2070 – Responsabilité de l'organisation en cas de recours à un prestataire externe pour ses activités d'audit interne

Lorsque l'activité d'audit interne est réalisée par un prestataire de service externe, ce dernier doit alerter l'organisation qu'elle reste responsable du maintien d'un audit interne efficace

Interprétation :

Cette responsabilité est démontrée par le programme d'assurance et d'amélioration qualité, lequel évalue la conformité avec la Définition de l'audit interne, le Code de déontologie et les *Normes*.

Le recours permanent à l'externalisation (pour tout ou partie du plan d'audit) est une décision stratégique à réviser périodiquement.

1.2.2- Motifs classiques de recours à des prestations externes

Généralement, les responsables de l'audit interne font appel à des prestataires pour en retirer les avantages suivants[11] :

- bénéficier d'expertises sans avoir à maintenir, en interne, l'ensemble des compétences nécessaires pour couvrir des domaines vastes, évolutifs et complexes tels que les SI ;
- respecter les échéances d'une mission ;
- intervenir dans des entités éloignées (intervenants locaux ou maitrisant la langue) ;
- remédier à une pénurie temporaire de personnel ;
- préserver l'objectivité et l'indépendance des auditeurs internes. Toutefois, le RAI devra également veiller à gérer les conflits d'intérêt liés aux prestataires externes (cf. partie 4).[12]

1.2.3- Facteurs limitants et inconvénients

Malgré ces avantages, le responsable de l'audit interne devra prendre en compte d'autres éléments pouvant influencer sa décision de recourir à une prestation externe et les modalités d'intervention :

- des coûts d'ajustement de l'approche du prestataire trop élevés ; en particulier pour l'audit de processus très spécifiques à l'organisation (RH, Achats, R&D…) ;
- des missions trop génériques, en définitive non crédibles et à faible valeur ajoutée pour les audités et leur management en raison d'une méthodologie inadaptée du prestataire ou d'un manque de connaissance de la culture, de l'environnement et des processus de l'organisation. Cette situation résulte souvent de l'absence de cahier des charges ou d'objectifs

[11] *CRIPP 2014 : MPA 1210. A1-1 « Recours à des prestations externes », Prise de position de l'IIA sur les ressources de l'audit interne (p.4)*

[12] *Guide Pratique : Indépendance et objectivité, p.12 - 13, Sous-traitance - IIA / IFACI, 2011*

© IFACI

d'audit suffisamment précis. Elle est amplifiée par un manque d'implication du service d'audit ou du management ;

- une moindre capacité à capitaliser le savoir-faire et l'expertise au sein de l'équipe d'audit interne ;
- le coût associé au type de prestation (expertise, récurrence, éloignement des sites à auditer) ;
- la maturité du service d'audit (programme d'assurance[13] qualité, compétences sur le domaine audité) ;
- la stratégie de gestion des ressources actée par les organes de gouvernance (cf. 2).

La décision du responsable de l'audit interne dépendra donc des orientations stratégiques de recours à des prestations externes définies au niveau du service d'audit et des dispositions particulières liées au type de mission.

[13] *CRIPP 2014 : MPA 1312-1 « Evaluations externes »*

© IFACI

Partie 2

Orientations concernant le recours à des prestations externes

Le recours ponctuel ou récurrent à des prestations externes devrait découler d'une décision argumentée du responsable de l'audit interne. Cette réflexion devrait répondre à des besoins stratégiques (cf. 2.1- Stratégie de gestion des ressources du service d'audit) ou opérationnels (cf. 2.2- Orientations pour la gestion des prestations externes au niveau d'une mission). Tout en renforçant la capacité de l'audit interne à contribuer à l'atteinte des objectifs de l'organisation, il s'agit de maîtriser des risques propres[14] au service d'audit (risque d'échec de l'audit, risque de donner une fausse assurance et risque d'atteinte à la réputation).

[10] *MPA 2120-2. Gestion du risque lié à l'activité d'audit interne*

© IFACI

2.1- Stratégie de gestion des ressources du service d'audit

C'est à partir du recensement des besoins et des compétences de l'audit interne que le responsable de l'audit interne choisira de mettre à niveau ses ressources internes (formation, recrutement…) et/ou de recourir à des ressources externes au service d'audit interne. Lorsqu'il décide de s'engager dans cette dernière option, le responsable de l'audit interne devra se poser un certain nombre de questions pour élaborer sa stratégie et la mettre en œuvre à travers une politique validée par les instances de gouvernance.

2.1.1- Détermination d'un modèle de gestion des compétences

La gestion des compétences devrait s'inscrire dans une vision à moyen et long terme. La stratégie[15] de l'audit interne se fonde sur un état des lieux et une analyse de l'évolution potentielle :

- des attentes des organes de gouvernance (y compris le rôle de l'audit interne dans la gestion des talents de l'organisation) ;
- des caractéristiques de l'organisation (niveau de centralisation/ décentralisation, périmètre géographique, métiers, risques à couvrir…) ;
- du budget du service d'audit (effectif, charges, flexibilité) ;
- des compétences générales (y compris linguistiques) et spécialisées.

C'est de la confrontation de ces besoins et des ressources internes existantes que le responsable de l'audit interne propose aux organes de gouvernance un plan de gestion des ressources (recrutement, formation, recours à des prestations externe) adapté à son contexte.

Pour en savoir plus

- Guide pratique : Elaborer le plan stratégique de l'audit interne / IIA / IFACI, juillet 2012
- Guide Pratique : Définir un processus de gestion des compétences / IIA / IFACI, avril 2015
- Rapports CBOK[16]

2.1.2- Définition d'une politique de recours à des prestations externes

La décision de s'engager dans le recours à des prestations externes relève d'un choix structurant pour le service d'audit interne. Il est donc recommandé de formaliser les options choisies dans une politique, validée par les instances de gouvernance, mise en œuvre et actualisée au fil des expériences (cf. 4.4) et de l'évolution des besoins.

[15] *Guide pratique : Elaborer le plan stratégique de l'audit interne / IIA / IFACI, Juillet 2012*

[16] *CBOK 2015 - Common Body of Knowledge - IIARF : Réussir dans un monde en mutation - dix impératifs pour l'audit interne, juillet 2015. Surfer sur les SI ; Le top 10 des risques SI - le rôle de l'audit interne, octobre 2015*

© IFACI

Bonne pratique

Le format de cette politique sera à adapter en fonction de l'organisation du service d'audit interne, de son système de documentation et de son niveau d'engagement dans le recours à des prestations externes.

Ainsi, cette politique pourra faire l'objet d'une section dans la politique globale de l'audit interne ou être référencée dans la politique globale mais donner lieu à un document à part entière avec des annexes facilitant le pilotage au niveau du service et au niveau de la prestation.

Cette politique résulte de plusieurs facteurs :

- d'un dialogue avec les instances de gouvernance ;
- de l'analyse des opportunités attendues et des risques à maîtriser au niveau de l'audit interne ;
- du contexte réglementaire et technique de l'organisation ;
- de l'univers d'audit.

2.1.2.1- Interagir avec les instances de gouvernance

Dans le cadre de ses relations hiérarchiques et fonctionnelles, le responsable de l'audit interne établit une relation étroite et régulière avec les instances de gouvernance (direction générale et Conseil / comité d'audit).

La décision de recourir à des prestations externes s'inscrivant dans la stratégie de l'audit interne doit être discutée avec ces instances de gouvernance afin de prendre en compte leurs attentes et obtenir leur approbation. Ce dialogue, conforme à la Norme 1110 « Indépendance dans l'organisation », est particulièrement important lorsqu'il s'agit d'externaliser des activités critiques pour l'audit interne ou que le taux d'externalisation est important.

Bonne pratique[17]

Les résultats de l'analyse du comité d'audit concernant les modalités de gestion des ressources de l'audit interne et son budget, devraient être consignés dans un procès-verbal. La recommandation du comité d'audit devrait être soumise, pour validation, au conseil d'administration ou à un autre organe de gouvernance.

Pour en savoir plus

- CBOK : Stakeholders study / IIARF (à paraître : https://global.theiia.org/iiarf/Pages/Common-Body-of-Knowledge-CBOK.aspx)

[17] *Prise de position de l'IIA sur les ressources de l'audit interne p.4*

2.1.2.2- Maîtriser les opportunités et les risques

Pour préparer les échanges avec les organes de gouvernance, le responsable de l'audit interne s'appuie notamment sur une revue des opportunités attendues des prestations externes et des risques pour le service d'audit, le tableau ci-dessous en donne quelques exemples. Il hiérarchise ces risques et opportunités en précisant leur niveau de maîtrise.

Objectif [18]	Exemples d'opportunité	Exemple de risques
Réduction des coûts	• Structure de coûts plus avantageuse (arbitrage coûts fixes vs coûts variables) • Budget annuel maîtrisé • Economies d'échelle	• Sous-estimation des coûts d'ajustement au contexte de l'organisation • Missions génériques à faible valeur ajoutée • Prestataires ayant une séniorité ou une expertise insuffisantes au regard des enjeux
Recentrage du service d'audit sur certaines missions correspondant par exemple, aux savoirs faire existants	• Meilleure utilisation des ressources internes • Avantage comparatif du prestataire pour la réalisation de certaines missions en co-traitance	• Limitation de la démarche de montée en compétence • Difficultés à capitaliser les retours d'expérience
Amélioration de la qualité	• Mise à profit des méthodes et des outils du prestataire • Transfert de compétences	• Surestimation de la plus-value de la méthodologie du prestataire • Sous-estimation des écarts entre les méthodes du prestataire et celles du service d'audit • Sous-estimation des prérequis et du coût du transfert de compétence • Sous-estimation des efforts en termes de supervision et d'accompagnement du prestataire
Couverture du périmètre de responsabilité	• Réalisation de missions sur l'ensemble des sites ou domaines concernés par les objectifs d'audit • Connaissance de la culture et de la langue locales	• Surestimation des capacités locales du prestataire

[18] *Guide Pratique : L'audit des relations avec les partenaires externes p.7 / IIA / IFACI, septembre 2009*

© IFACI

Objectif	Exemples d'opportunité	Exemple de risques
Respect des délais	• Accès à un ensemble de ressources, y compris humaines, plus réactif et flexible • Savoir plus approfondi et étendu, permettant de développer et de mettre en œuvre des programmes de travail plus efficaces	• Sous-estimation des temps de préparation, de coordination, de pilotage et de suivi des recommandations • Manque d'anticipation des ressources internes et externes nécessaires
Augmentation des ressources	• Vivier de talents plus large et flexible • Accès à de meilleures technologies et compétences	• Sous-estimation des coûts • Manque d'anticipation permettant une disponibilité effective des ressources en temps voulu • Sous-estimation du rôle de supervision de l'audit interne et de sa responsabilité ultime pour le portage des conclusions et des recommandations

Comme tout manager, le responsable de l'audit interne met en place un dispositif de maîtrise de ses services en veillant[19] :

- au respect des Normes internationales pour la pratique professionnelle de l'audit interne ;
- à l'adéquation du programme d'assurance et d'amélioration qualité de l'audit interne (Norme 1300), en particulier les procédures de supervision ;
- à une définition pertinente des domaines clés à auditer (connaissance de l'organisation, évaluation des risques « réels » de l'organisation et de l'efficacité des contrôles en place) ;
- à l'exercice du scepticisme professionnel des auditeurs.

En outre, les avantages des prestations ne seront effectifs qu'avec une préparation précise de chaque type de mission (cf. 2.2), de chaque contrat (cf. 3) ainsi qu'un suivi rigoureux de leur exécution (cf. 4).

2.1.2.3- Prendre en compte le contexte réglementaire et technique

Le responsable de l'audit interne doit également prendre en compte les contraintes réglementaires (par exemple, les exigences de traçabilité des travaux d'audit ou de gestion de la relation avec les clients ; l'existence de domaines sensibles ou de recommandations des instances de régulation sectorielle sur l'audit interne[20]) et techniques (métiers et stratégie de l'organisation, environnement du SI, politique d'achat …) de l'organisation.

[19] *MPA 2120-2*

[20] *Recommandations du comité de Bâle : www.bis.org*

© IFACI

Exemples de facteurs liés à l'environnement des SI à prendre en compte[21] :

- le niveau de centralisation ou de répartition des ressources SI ;
- les technologies déployées ;
- le degré de customisation ;
- le degré de formalisation des politiques et référentiels de l'organisation (gouvernance des SI, par exemple) ;
- le degré de réglementation et de conformité ;
- le degré et le mode d'externalisation ;
- le degré de standardisation des opérations ;
- le degré de dépendance technologique.

Point d'attention : Les revues externes réalisées à la demande de la DSI

Toute fonction peut directement recourir à des prestations externes. C'est particulièrement le cas de la DSI.

L'audit interne devra avoir accès aux revues externes réalisés à la demande la DSI. Lorsqu'il juge que ces travaux sont objectifs et fiables, le responsable de l'audit interne peut les prendre en compte pour étayer ses constats.

2.1.2.4- Couvrir l'univers d'audit

Une politique efficace de recours à des prestations externes contribue à une couverture efficace de l'univers d'audit. Ce dernier est défini à partir du périmètre de responsabilité fixé dans la charte de l'audit interne (cf. Norme 1000 « Mission, pouvoirs et responsabilités »). A partir de la structure de l'organisation (entités juridiques, métiers, fonctions,…) et des processus qui sous-tendent ce périmètre, le responsable de l'audit interne détermine les risques à couvrir et la périodicité associée.

En pratique : Comment assurer la couverture des risques SI quand il n'y a pas d'expert SI au sein de l'audit interne ?

- commencer par des « sujets triviaux ». L'entrée « métier » (accès, continuité, projets) est accessible à des auditeurs non spécialistes en SI qui peuvent dégrossir les sujets. Cette première analyse permettra de faire appel à des experts externes pour des points plus précis. Leur prestation en sera d'autant mieux cadrée et suivie ;
- se servir des observations des commissaires aux comptes pour le cadrage ;
- explorer les bonnes pratiques professionnelles (GTAG notamment) ;
- lorsque l'objectif d'audit est identifié, l'approfondir dans le cadre de pré-consultation d'experts externes (RFP-Request for proposal) ou internes.

[21] *Global Technology Audit Guide (GTAG) 11 : Elaboration d'un plan d'audit des SI. p.6 à 9 / IIA / IFACI, Juillet 2008*

© IFACI

2.1.3- Déclinaison opérationnelle de la politique

La politique de recours à des prestations externes d'audit est précisée par des procédures de sélection, de documentation et de communication (cf. partie 3).
Leur mise en œuvre est régulièrement revue (suivi des clauses contractuelles, supervision des travaux, cf. partie 4).
L'anticipation des étapes critiques que sont la renégociation du contrat et la réversibilité de la prestation est un facteur clé de succès.

2.2- Orientations pour la gestion des prestations externes au niveau d'une mission

Après avoir défini la politique du service d'audit interne en matière de recours à des prestations externes, il convient de se poser la question des orientations souhaitées au niveau de chaque mission concernée.
La formalisation du besoin servira à l'identification des ressources nécessaires (niveau d'expertise, expérience, méthodes et outils…) à l'exécution de la mission. Le responsable de l'audit interne s'appuiera sur cette analyse pour décider de recourir ou non à une prestation externe.

2.2.1- Spécifications de la mission

Il est nécessaire d'avoir une compréhension claire des besoins en lien avec les objectifs de la mission. Le responsable de l'audit interne s'assurera que les éléments suivants sont définis :

- Quels sont les principaux risques à couvrir ?
- Quel est le périmètre de la mission (domaines fonctionnels et techniques de l'intervention, parties prenantes, implantations concernées par les travaux de terrain) ?
- S'agit-il d'une mission d'audit SI experte ou d'un volet SI d'une mission généraliste ?
- La mission s'inscrit-elle dans le cadre d'une externalisation totale, d'une sous-traitance ou d'une co-traitance (cf. 1.2.1) ?
- Quelles sont les étapes clés de la mission et le planning envisagé ?
- La méthodologie de l'audit interne est-elle suffisante au regard des objectifs de la mission ?
- Existe-il un programme de travail standard ? Doit-il être adapté ?
- Quelles sont les expertises et outils nécessaires à la mise œuvre du programme du travail ?

Les réponses à ces questions donneront au responsable de l'audit interne des clés pour l'identification des ressources nécessaires à la conduite de la mission (constitution de l'équipe, méthodes et outils…).

© IFACI

2.2.1.1- Constitution de l'équipe

Les spécifications définies ci-dessus permettent d'identifier des profils adaptés à chaque type de mission. Ces profils sont illustrés dans le tableau suivant à partir de la typologie définie dans la partie 1.1. La connaissance des fondamentaux de l'audit des SI est un prérequis. L'unité de recherche a mis l'accent sur deux critères définis comme suit :

- Niveau de séniorité :
  - A : Débutant (1 à 3 ans),
  - B : Intermédiaire (4 à 10 ans),
  - C : Elevé (10 ans +)
- Niveau d'expertise :
  - 1 : Compétent pour effectuer une évaluation générique
  - 2 : Connait suffisamment un domaine ou une technologie pour réaliser certaines tâches avec une supervision limitée
  - 3 : Maîtrise un domaine ou une technologie et réalise des tâches complexes

Ces niveaux sont donnés par convention, ils sont à adapter en fonction des circonstances. De même les critères peuvent être affinés pour se focaliser sur des compétences de savoir-faire (exemple : analyse de données) ou de savoir-être (communication) spécifiques.

Point de vigilance

In fine, quel que soit le niveau d'externalisation décidé par le RAI, il devra prévoir un minimum de ressources internes pour le pilotage de la mission.
En outre, la connaissance des fondamentaux de l'audit des SI est un atout voire un prérequis pour certaines missions.

© IFACI

Types de mission [22]	Spécifications [23]	Profils
Audit de la gouvernance des SI	• Compréhension des enjeux, des métiers et du fonctionnement de l'organisation. • Capacité à susciter l'adhésion des décideurs. • Forte implication de l'audit interne en particulier lors des entretiens avec les dirigeants. • Capacité à proposer des recommandations à valeur ajoutée et adaptées au contexte.	Niveau de séniorité : C Niveau d'expertise : 1 ou 2
Audit de la gouvernance des SI – *Cas particulier : audit des infrastructures*	• Capacité à interpréter la cartographie des éléments d'infrastructure (réseau, base de données, serveurs, unités de stockage, hébergement…) de l'organisation. • Le cas échéant, compréhension des enjeux d'un contrat de services externalisés (par exemple, en matière de *cloud computing*).	Niveau de séniorité : B Niveau d'expertise : 3
Audit de la gouvernance des SI – *Cas particulier : audit des prestations informatiques externalisées*	• Bonne connaissance des ressources informatiques (actuelles, futures) de l'organisation. • Expérience de la gestion contractuelle et de la revue de contrat et SLA (*Service Level Agreement* ou contrat de niveau de service). • Maîtrise des éléments liés à la protection des données externalisées. • Capacité à évaluer l'efficience des prestations (benchmark des coûts des prestations, des offres de service). • Le cas échéant, connaissance de la réglementation sectorielle.	Séniorité : B ou C Expertise : 1 ou 2

[22] *Tels que présentés au § 1.1.*

[23] *Les spécifications indiquées dans ce tableau n'ont pas l'ambition d'être exhaustives. Elles donnent quelques pistes pour déterminer le profil adapté*

© IFACI

Types de mission	Spécifications	Profils
Support à la revue de processus opérationnels et fonctionnels – *analyse de données et contrôle en continu*	• Connaissance des processus métiers de l'entité et du secteur d'activité indispensable, ainsi que la maitrise du contrôle interne informatique. • La capacité à partager des bonnes pratiques concernant les ERP, du type SAP, Oracle, Microsoft, etc. • Méthodologies de revue des processus (catalogues de contrôles automatiques, semi-automatiques, états d'exceptions et catalogues d'indicateurs de risque et de performance). • La maitrise des outils d'analyse de données permet de renforcer l'opinion (automatisation des traitements, exhaustivité des analyses et qualité des synthèses). • En fonction des analyses souhaitées (prédictives ou détectives), de la volumétrie des données, de la sophistication du SI et du type de données (structurées ou non-structurées), l'intervention d'experts dans les bases et les modèles de données peut être requise.	Séniorité : B ou C Expertise : 2 ou 3
Support à la revue de processus opérationnels et fonctionnels – *Contrôles applicatifs*	• Connaissance des processus métiers de l'entité et du secteur d'activité indispensable, ainsi que la maitrise du contrôle interne informatique. • Expérience validée de la revue de des contrôles automatiques « embarqués » dans le SI. • La capacité à partager des bonnes pratiques concernant les ERP, du type SAP, Oracle, Microsoft, etc. • Méthodologies de revue des processus (catalogues de contrôles automatiques, semi-automatiques, états d'exceptions et catalogues d'indicateurs de risque et de performance).	Séniorité : B ou C Expertise : 3
Contrôles généraux informatiques (relatifs à des applications ou à des infrastructures SI) – *Régularité et conformité*	• Maitrise des enjeux réglementaires et de conformité propres à l'organisation. • Veille réglementaire et expertise en fonction des sujets à traiter (Cconformité fiscale, protection des données personnelles, loi anti-blanchiment, conformité comptable…). • Une expertise de la conformité sectorielle est aussi nécessaire (Loi transparence dans le domaine pharmaceutique, Bale2 dans le domaine Bancaire, Solvency2 dans le domaine Assurance…). Tous les domaines d'activité ont leurs propres problématiques sectorielles réglementaires. • Un support d'experts « locaux » peut être requis pour des enjeux réglementaires à l'international.	Séniorité : B ou C Expertise : 1 à 3

© IFACI

Types de mission	Spécifications	Profils
Contrôles généraux informatiques (relatifs à des applications ou à des infrastructures SI) – *Projets (développement, gestion des changements)*	• Maitrise des organisations SI, des études informatiques et des processus des DSI. • Certaines certifications sont utiles voire nécessaires : CISA (Certified IS Auditor), PMI ou Prince2 (gestion de projet), ITIL (qualité des services de la DSI). • Dans le cas d'une revue détaillée de la sécurité et de la qualité des développements, des notions dans les principaux langages de programmation peuvent être nécessaires.	Séniorité : B ou C Expertise : 2 ou 3
Contrôles généraux informatiques (relatifs à des applications ou à des infrastructures SI) – *Sécurité*	• Apport si possible de programmes de travail experts en fonction des technologies de l'entité. • Maitrise du référentiel ISO 27002. • Une attention particulière sur le sujet Cyber sécurité (connaissance des outils d'*ethical hacking ;* maitrise des approches de tests d'intrusion).	Séniorité : B ou C Expertise : 3
Contrôles généraux informatiques (relatifs à des applications ou à des infrastructures SI) – *Accès logiques et physiques*	• Apport si possible de programmes de travail experts en fonction des technologies de l'entité. • Maitrise du référentiel ISO 27002. • En fonction du périmètre de la mission (sécurité des systèmes d'exploitation, des réseaux, des bases de données, des applications, sécurité physique…), les expériences et la maitrise des principes de sécurité du domaine visé doivent être privilégiées.	Séniorité : A ou B Expertise : 2 ou 3
Contrôles généraux informatiques (relatifs à des applications ou à des infrastructures SI) – *Production / exploitation*	• Certaines expertises techniques peuvent être nécessaires en fonction des outils de l'organisation (Systèmes de sauvegardes, consoles d'exploitation. • Maitrise du référentiel ITIL et expérience de son application dans le cadre ITSM (IT Service Management).	Séniorité : A ou B Expertise : 2 ou 3
Contrôles généraux informatiques (relatifs à des applications ou à des infrastructures SI) – *Support utilisateurs*	• Maitrise indispensable du référentiel ITIL et expérience de son application dans le cadre ITSM (IT Service Management). • Plusieurs facteurs de complexité peuvent être notés nécessitant des profils très expérimentés en cas de sous-traitance du support utilisateurs, de la mise en place de niveaux de service et d'analyse des coûts détaillés.	Séniorité : B ou C Expertise : 1 ou 2
Contrôles généraux informatiques (relatifs à des applications ou à des infrastructures SI) – *Plan de secours*	• Type de mission très complexe nécessitant une connaissance à la fois de l'organisation, des risques, des processus métiers et de l'environnement informatique. • Expertise sur les domaines (gestion des crises, mécanismes de redondance informatique, etc.).	Séniorité : C Expertise : 2 ou 3

© IFACI

Pour chaque mission, le profil requis sera à adapter en fonction du niveau d'interaction au sein de l'organisation (par exemple, l'interaction avec des dirigeants impactera le niveau de séniorité). En fonction de la constitution de l'équipe et des compétences, il conviendra d'avoir une vue claire du planning des intervenants. A ce stade, les différents profils (niveau d'expertise, niveau d'expérience) peuvent être identifiés en interne ou complétés par des ressources externes.

2.2.1.2- Méthodes et outils requis

Pour chacune des missions présentées, il sera attendu que le prestataire propose une démarche d'audit quand celle-ci n'existe pas ou est insuffisante en interne. C'est aussi l'occasion d'avoir un regard critique sur les approches d'audit interne. L'apport méthodologique doit avoir lieu dès la phase de préparation.
Les experts pourront intervenir avec leurs propres outils (par exemple, pour de l'analyse de données, de l'analyse des autorisations, la réalisation de tests d'intrusion, ou pour le suivi de l'audit, etc.). Il convient de s'assurer d'une part que les licences des outils du prestataire permettent une telle intervention et, d'autre part, que des risques d'effets de bord techniques sur le SI de l'organisation sont maîtrisés (par exemple via une validation pour la DSI).
Le niveau de documentation attendu durant et à l'issue de l'intervention devra être précisé.

2.2.2- Prise de décision

La décision du responsable de l'audit interne se fondera sur une synthèse de l'évaluation des besoins (cf. 2.1) et des facteurs limitants (cf. 1.2.3).
Soit le responsable de l'audit interne décide de ne pas faire appel à des prestations externes parce qu'il considère, notamment que :

- les compétences disponibles au sein de l'audit internes sont suffisantes[24] ;
- le programme de formation permettra de combler les lacunes ;
- des experts internes (par exemple de la DSI) peuvent être mobilisés en maîtrisant les risques d'atteinte à l'indépendance et à l'objectivité ;
- le budget pour des prestations externes n'est pas disponible…

Soit il s'engage vers un recours à des prestations externes. La définition des objectifs de la mission et des ressources internes permettront alors de préciser les compléments attendus de la part du prestataire en termes :

- de compétences techniques (exemple : experts ERP, experts cyber sécurité…) ;
- d'effectifs pour élargir le périmètre d'intervention ;
- de méthodologie (maitrise du COBIT ou des Normes ISO 27000) ou d'outils (outils de tests de pénétration réseau ou d'analyse de données…) ;

[24] *Guide pratique : Définir un processus de gestion des compétences / IIA / IFACI, Avril 2015*

© IFACI

- La décision d'externalisation prise, l'implication du prestataire devra être adaptée à chaque contexte. Selon la typologie proposée en partie 1.2, elle pourra consister en :
  - une sous-traitance : l'équipe externe est mobilisée sous la supervision de l'audit interne ;
  - une co-traitance : les experts externes sont entièrement intégrés dans une équipe interne encadrée par un chef de mission interne ;
  - une co-traitance : les intervenants externes réalisent des travaux de préparation et d'analyse en chambre pour faciliter le travail de l'équipe d'audit interne. La phase terrain étant réalisée en commun.

Le niveau d'implication de l'audit interne dans la supervision des travaux est un point d'attention particulièrement important. De même que l'implication des managers et experts externes est déterminante pour l'encadrement des équipes et la revue des livrables. Elle garantit la qualité des travaux et le niveau d'expertise attendue.

© IFACI

© IFACI

Partie 3

Modalités pratiques d'engagement d'un prestataire

Lorsque la décision de s'engager dans le recours à des prestations externes est prise (cf. partie 2 : Orientations concernant le recours à des prestations externes), il convient d'en préciser les modalités pratiques : comment sélectionner le prestataire (cf. 3.1- Mise en concurrence et sélection du prestataire) ? Quels sont les incontournables du contrat (cf. 3.2- Contractualisation) ?

© IFACI

3.1- Mise en concurrence et sélection du prestataire

La mise en concurrence, même lorsqu'il ne s'agit pas d'une contrainte réglementaire, constitue une bonne pratique permettant d'améliorer la pertinence et l'efficience du recours aux prestations externes. C'est pourquoi, l'unité de recherche a décidé d'en rappeler ci-après les points clés.

3.1.1- Mise en concurrence : les points essentiels de l'appel d'offres

La mise en concurrence des prestataires de services (cabinets d'audit, sociétés spécialisées en sécurité informatique, en plan de continuité d'activités, en gestion de projets, etc.) peut se faire soit à partir d'une liste restreinte de prestataires, soit être ouverte. Le choix d'une liste restreinte peut se justifier par des contraintes de délais, par le référencement des prestataires, ainsi que par le niveau de sensibilité des informations figurant dans le cahier des charges.

3.1.1.1- Principes généraux de recours à des services intellectuels

La sélection d'un fournisseur diffère selon qu'il s'agisse d'un marché public ou d'une mise en concurrence initiée par une organisation privée dans le cadre de sa politique de gestion des achats. Cependant, il s'agit toujours de sélectionner l'offre la plus efficiente, de promouvoir la transparence et de maîtriser les comportements non-éthiques.

Pour mémoire, les principes fondamentaux de la commande publique (art.1 CMP : Code des Marchés Publics[25]) sont les suivants :

- la liberté d'accès à la commande publique ;
- l'égalité de traitement des candidats ;
- la transparence des procédures ;

Ces bonnes pratiques peuvent également être appliquées dans le secteur privé. En outre, l'article 26 du CMP définit des seuils et des procédures de passation des marchés publics.

3.1.1.2- Modalités opérationnelles de réalisation de l'appel d'offres

Même lorsqu'il ne s'agit pas d'une exigence réglementaire, l'appel d'offres est un moyen efficace pour effectuer un choix optimal d'un prestataire de service. Par la comparaison objective et méthodique des offres, les meilleures propositions devraient pouvoir être obtenues au meilleur prix.
On distingue généralement 6 étapes dans le processus classique d'un appel d'offres. Ce processus devra, le cas échéant, répondre aux exigences légales. Il peut être simplifié en fonction des enjeux :

[25] http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000005627819

© IFACI

a) Rédaction du cahier des charges

La préparation d'un appel d'offres commence avec l'élaboration d'un cahier des charges, qui décrit généralement :

- le contexte ;
- les enjeux ;
- les objectifs ;
- les exigences ;
- les attentes.

Exemple de précisions pouvant être mentionnées dans un cahier des charges

- respect des politiques et procédures de l'organisation ;
- secret professionnel, respect de la propriété intellectuelle et confidentialité des informations / données (métiers, techniques ou encore la localisation des salles hébergeant les serveurs de l'organisation) qui seront traitées ;
- connaissance du contexte règlementaire (SOX, Bâle II, LSF, etc.) ;
- livrables attendus ;
- modalités d'exécution de la prestation. Par exemple :
  - co-traitance éventuelle ;
  - planning d'intervention ;
  - langue (s) de travail ;
  - périmètre géographique d'intervention…

Pour les domaines où le responsable de l'audit interne considère que les compétences présentes dans son service sont insuffisantes, il peut demander l'avis d'experts internes (responsable de la sécurité du système d'information (RSSI), collaborateur de la Direction des Systèmes d'Information-DSI…) à condition de maîtriser les risques d'atteinte à leur objectivité. L'avis d'experts externes peut être sollicité, par exemple dans le cadre d'un processus de présélection *(Request for proposal)*.

b) Définition des critères de sélection

Il s'agit de définir les méthodes d'analyse des offres et de formaliser des grilles de sélection avec des critères tels que :

- les éléments de la décision de recourir à un prestataire et qui permettent d'évaluer la qualité technique de l'offre (cf. 2.2) ;
- le coût ;
- les langues ;
- les caractéristiques du soumissionnaire (relais dans les zones géographiques concernées par la mission, expériences et références sur le sujet, certifications professionnelles…).

Bien entendu, ces critères devront être cohérents avec la politique d'achat de l'organisation.

© IFACI

c) Choix des soumissionnaires et diffusion de l'appel d'offres

Le choix des soumissionnaires est une présélection des prestataires potentiels sur le marché susceptibles de couvrir les besoins du service d'audit interne exprimés au travers du cahier des charges. Cette présélection a pour avantage de limiter le nombre de prestataires et donc la charge de traitement des offres. Néanmoins, par soucis d'exhaustivité ou du fait d'une méconnaissance du marché, certains responsables de l'audit interne préfèrent procéder à des appels d'offres ouverts.

Les documents d'appel d'offres comportent généralement les rubriques suivantes :

- description de l'organisation délégante ;
- déroulement de l'appel d'offres (processus de sélection, réunions d'informations, échéances des réponses …) ;
- cahier des charges des prestations attendues ;
- dates de livraison ;
- grille de cotation commune des prestataires ;
- contacts clés ;
- engagement des soumissionnaires ;
- formulaire d'accusé de réception.

d) Réception, analyse des offres et évaluation des soumissionnaires

Les réponses des prestataires au cahier des charges sont réceptionnées et analysées par le responsable de l'audit interne, qui impliquera les collaborateurs qui seront amenés à suivre les travaux et la prestation.
Une grille de sélection, qui tiendra compte des critères définis dans la politique d'achat de l'organisation, facilitera la consolidation et la comparaison objective des réponses des soumissionnaires sur des points tels que l'expérience, les compétences, la pertinence de l'offre technique, etc.

e) Soutenance orale

Cette étape est cruciale dans le processus de sélection du prestataire. C'est le lieu pour le responsable de l'audit interne (accompagné éventuellement par des experts indépendants ou des représentants du service achat) d'interroger les soumissionnaires, retenus à l'issue de l'évaluation de leurs offres techniques et financières. Certaines informations notamment les certifications professionnelles, les références et expériences pertinentes des prestataires sont vérifiées et confirmées.

f) Choix du prestataire et contractualisation

Il s'agit de la dernière étape du processus d'appel d'offres. Le responsable de l'audit interne sélectionne le prestataire qui signera un contrat avec l'organisation.

© IFACI

3.1.2- La sélection du prestataire

Les conclusions de l'analyse des risques et des opportunités associés au recours à un prestataire (cf. 2) déterminent le processus de sélection.

3.1.2.1- Impact de la nature et du contexte de la mission

Les principaux facteurs ayant un impact sur la sélection d'un prestataire externe sont :

- le domaine d'activité (banque, sécurité nationale, aéronautique, assurance, etc.) ;
- la nature de la mission (cf. 2.2) ;
- la culture de l'organisation (taux de recours aux prestataires externes) ;
- les bonnes pratiques professionnelles d'audit interne[26] avec, notamment :
  - la capacité du prestataire (compétences, qualifications professionnelles dans le domaine à auditer, agréments éventuels, effectifs, outils) ;
  - l'expérience du prestataire dans le domaine à auditer (exemple de missions, références de clients) ;
  - l'indépendance et l'objectivité du prestataire ;
  - le professionnalisme du prestataire (méthodologie, éthique et déontologie)...

3.1.2.2- Evaluation des offres

L'évaluation des éléments fournis par les soumissionnaires reflète l'analyse des risques et opportunités de la prestation (cf. partie 2) ainsi que les critères qualitatifs et quantitatifs établis lors de la rédaction de l'appel d'offres.

a) Les critères qualitatifs

Le Cadre de référence des pratiques professionnelles de l'IIA[27] propose plusieurs éléments à prendre en considération, et à moduler selon la nature de la mission et le contexte de l'organisation, parmi lesquels :

>> l'indépendance et l'objectivité des intervenants

Au regard des bonnes pratiques d'achat et d'audit, la vérification de l'indépendance et de l'objectivité du prestataire est primordiale. Pour bénéficier d'un jugement professionnel et objectif, le responsable de l'audit interne devra être attentif :

- à la nature des prestations déjà fournies à l'organisation. Par exemple, un prestataire qui serait intervenu pour la définition ou la mise en place des politiques et procédures liées à la sécurité du système d'information pourrait difficilement être retenu pour une mission sur le même domaine ;

[26] *Cf. CRIPP 2014 : MPA 1210.A1-1*

[27] *Prise de position de l'IIA sur les ressources de l'audit interne, MPA 1210 A1-1*

© IFACI

- aux relations personnelles ou professionnelles des prestataires avec des membres de l'équipe d'audit interne ou d'autres collaborateurs de l'organisation ;
- aux principes déontologiques de certaines professions. Par exemple, « même si la législation ou la réglementation l'autorise, l'IIA déconseille aux organisations de confier des activités d'audit interne au cabinet d'audit externe qui vérifie leurs états financiers, car cela porterait atteinte au principe d'indépendance.»[28] ;
- aux intérêts économiques tels que la possession d'actions ;
- aux intérêts commerciaux (par exemple au travers de conclusions d'audit permettant de positionner des missions de conseil ou d'accompagnement post audit) ;
- aux préjugés raciaux, culturels ou fondés sur le genre ;
- aux modalités de rémunération liées à la réalisation de la prestation.

Les risques d'atteinte à l'objectivité et à l'indépendance ne sont pas toujours évidents à mesurer surtout lorsqu'il s'agit des relations personnelles. Il convient néanmoins de les prévenir (prise en compte lors de la rédaction de l'appel d'offres, déclaration d'indépendance et d'objectivité signée par les membres de l'équipe du prestataire) et de les maîtriser (entretiens avec les membres de l'équipe du prestataire...).

>> Compétence et qualifications

Le prestataire externe doit pouvoir démontrer de réelles capacités professionnelles non seulement en audit, en gouvernance et en sécurité des SI, mais aussi en gestion des projets et en communication. Des critères objectifs d'évaluation de ces exigences sont proposés dans le tableau ci-après. Ils font écho aux critères de séniorité et d'expertise présentés dans la partie 2.2. Ils peuvent être applicables à tous les membres de l'équipe ou uniquement au personnel clé.

Bonne pratique

Pour faciliter la revue des offres et le suivi de la prestation, il convient de définir précisément les critères d'éligibilité pour chaque rôle clé de la mission.

Rappelons que la compétence soutient l'objectivité. Un auditeur incompétent peut être tenté de biaiser ses travaux ou ses conclusions afin de masquer ses lacunes. En outre, c'est un élément important à prendre en considération s'il est prévu un transfert de compétence du prestataire vers l'audit interne.

[28] *Prise de position de l'IIA sur les ressources de l'audit interne.p.5*

© IFACI

Critère	Description / Exemples
Formation initiale	Masters en système d'informations (audit, sécurité, gouvernance). Formations en ingénierie informatique.
Affiliation et activités au sein d'associations professionnelles	L'appartenance et la participation aux activités de l'IIA ou de l'IFACI ou encore de l'ISACA (représenté par l'AFAI en France) indiquent la volonté de se tenir à jour des meilleures pratiques professionnelles.
Formations internes chez le prestataire	Elles permettent de maintenir à jour les compétences et de rester pertinent malgré les évolutions technologiques.
Connaissances règlementaires	Si la prestation s'inscrit dans le cadre d'une règlementation (par exemple SoX, HIPAA, etc.), des formations spécifiques liées à ces règlementations fournissent une assurance supplémentaire sur la compétence du prestataire.
Précurseur et pédagogue	La participation à la rédaction de publication et d'articles dans le domaine est une indication de la maitrise du domaine, de la capacité à rendre compte de son expérience et à partager ses connaissances.

>> Professionnalisme

La référence à des normes reconnues, l'adhésion à un code de déontologie et la méthodologie propre au cabinet (y compris le processus de contrôle qualité) constituent un gage de professionnalisme.

En matière de déontologie, le service d'audit interne devra particulièrement être attentif au respect des règles de l'IIA (intégrité, objectivité, confidentialité, compétence). Par exemple, il y a des risques de non maîtrise de la confidentialité du fait de l'accès à des fichiers et des configurations sensibles (adresses IP, ports ouverts, protocoles, fichiers de mots de passe cryptés, etc.) et à des données sensibles (données personnelles, financières, liées à la stratégie…). Au-delà d'un engagement de confidentialité, le responsable de l'audit interne devra s'assurer de la présence d'outils sécurisés sur les postes des prestataires et définir des protocoles d'accès et de manipulation des données qui soient a minima conformes à ceux existants dans l'organisation.

>> Références et réputation

Ces éléments permettent d'estimer la capacité du prestataire à mobiliser des compétences sur le domaine concerné. L'évaluation de cette capacité peut d'ailleurs être corroborée par d'autres informations fournies par le prestataire, comme par exemple ses outils.

L'évaluation des références se fait au niveau du prestataire de service (par exemple, missions antérieures dans l'audit des ERP) mais également, et surtout, par la confirmation que des intervenants expérimentés dans le domaine seront bien engagés dans la mission.

Les réseaux sociaux de professionnels constituent des outils utiles pour croiser les informations. Des prises de contact plus directes par mél ou téléphone dans les entreprises référencées sont tout aussi usuelles. Par ailleurs, la connaissance d'une autre référence non mentionnée dans la

© IFACI

réponse à l'appel d'offres est une occasion d'avoir des avis nuancés sur la capacité du prestataire à délivrer dans les délais et avec la qualité requise.

>> Communication

L'aptitude du prestataire à communiquer avec le service d'audit interne et les audités est également un facteur clé de succès de la mission.
Une intégration, dans l'organisation et dans le service d'audit, mal gérée par le prestataire, peut entrainer des perturbations. L'enjeu pour le service d'audit interne est d'autant plus important que les phases critiques de l'intervention nécessitent beaucoup d'interactions et de coordination. De plus, la complexité des SI nécessite souvent l'implication de divers acteurs tant au sein de la DSI que des directions métiers. Par conséquent, la maîtrise de la communication est cruciale.

>> Autres critères

D'autres critères qualitatifs peuvent être pris en compte :

- la capacité à mobiliser et rendre disponible des ressources de bon niveau et la flexibilité de la dotation en personnel pour faire face aux objectifs de la mission ou à des demandes spéciales découlant des travaux préliminaires ;
- l'apport d'outils (analyse de données notamment du Big data, documentation des travaux, diagnostics de sécurité…) ;
- la capacité à couvrir des sites éloignés ;
- l'implication du personnel clé (implication du représentant du prestataire niveau de séniorité de l'équipe…) ;
- taux de rotation du personnel chez le prestataire.

L'évaluation de ces critères qualitatifs comprend une part de jugement professionnel. C'est pourquoi elle doit être faite par une équipe de personnes expérimentées et habituées à l'exercice. Bien que pilotée par l'audit interne, l'implication de la direction des achats dans cette évaluation peut être envisagée.

b) Les critères quantitatifs

L'analyse des critères quantitatifs de coûts et de délais permettent de compléter l'analyse qualitative dans le processus de sélection. S'ils sont plus aisés à objectiver, ces critères ne doivent pas masquer les aspects qualitatifs.

>> Coûts

La structure des coûts proposée par le prestataire devra être analysée avec attention. Ainsi, les taux horaires des consultants doivent être appréciés au regard de la séniorité, de la compétence et de l'expérience dans le type de prestation.

© IFACI

L'optimisation du mode de facturation doit également être recherchée. Dans un schéma simple, le prestataire peut être facturé selon un forfait qui peut inclure les débours et les honoraires. Un forfait inclusif peut paraître plus avantageux puisque le prestataire serait seul responsable des dépassements de débours à moins de renégocier le budget. Les zones géographiques d'intervention et l'implication des équipes locales du prestataire sont à prendre en compte dans cette analyse.

Ils convient également d'apprécier les coûts cachés de la prestation. Par exemple, les coûts de supervision.

>> Durée d'exécution des travaux

La capacité du prestataire à délivrer la prestation attendue dans les délais requis est influencée par certains critères qualitatifs mentionnés ci-dessus comme la méthodologie utilisée, les tests à réaliser, les compétences disponibles (effectifs du prestataire, expérience et compétences des équipes mobilisées).

En pratique
Pour faciliter l'analyse, une grille de notation et de pondération correspondant à ces différents critères peut être utilisée.

3.2- Contractualisation

Le recours à des prestations externes comporte des risques inhérents (cf. 2.1.2.2) et des risques spécifiques liés au prestataire choisi. Le contrat doit donc être établi avec soin et refléter la stratégie d'externalisation (cf. 2.1) et les moyens à engager (Cf. 2.2 et 3.1).
Pour le prestataire sélectionné, le contrat permet de définir avec précision la nature et l'étendue de son intervention au regard d'un prix convenu, souvent forfaitaire.
Pour le responsable de l'audit interne, l'enjeu n'est pas moindre puisqu'il s'agit de préciser les attentes vis-à-vis du prestataire ainsi que les responsabilités tout au long de la mission.
Le contrat introduit donc le cadre nécessaire à l'exécution et à la supervision de la mission (cf. 4), en particulier sur les aspects méthodologiques mais également sur des éléments très spécifiques comme la propriété des dossiers de travail.
Le contrat pourra également prévoir des obligations et des garanties que le prestataire s'engagera à respecter. En ce sens, il limite les risques de litiges.
Le succès de la contractualisation dépendra de la qualité de l'appel d'offres, ainsi que de la précision des services attendus et des prérequis à la prestation.

© IFACI

Point d'attention

Pour avoir accès à un pool d'expertises pointues susceptibles de répondre à la diversité des sujets à auditer, le responsable de l'audit interne peut autoriser le recours à des prestataires de second ordre. Les modalités de ce recours devront être formellement précisées avec le contractant principal.

3.2.1- Eléments à prendre en considération

Le choix d'externaliser une mission d'audit comporte des risques (cf. 2.1.2.2) qu'il convient de gérer dès la sélection du prestataire, mais également lors de la formalisation du contrat en clarifiant notamment les rôles et responsabilités, l'étendue et limites des travaux, leurs modalités de réalisation et de contrôle, les éventuelles pénalités et les conditions de renouvellement de la prestation. Cette anticipation est d'autant plus indispensable que les sujets SI sont transverses et que la mission peut avoir des répercussions qu'il faut savoir prévoir et maitriser.

Le niveau d'implication du prestataire à chaque étape de la mission est à préciser, depuis la définition du périmètre et des objectifs jusqu'à la restitution des conclusions (une lettre de mission pourra être annexée au contrat). Il convient de ne pas omettre les objectifs connexes tel que le transfert de compétences du prestataire vers le service d'audit interne. Celui-ci peut, par exemple, se faire à travers de la co-traitance ou par la formalisation d'un guide d'audit complet pour le domaine audité. Le transfert de compétences sera probablement limité pour des audits informatiques techniques mais pourra être plus élevé pour des missions portant sur la gouvernance du SI ou sur des revues de projets informatiques.

Il est important également d'identifier contractuellement le représentant légal du prestataire voire le chef de projet afin de clarifier le circuit d'échanges et de communication entre les parties. La responsabilité individuelle de chaque membre de l'équipe de prestataires et celle des signataires de la lettre de mission devront également être précisées.

Le contrat devra prendre en compte les modalités d'intégration du prestataire. En effet, le prestataire pourra réaliser la mission de façon indépendante, avec la production d'un rapport ad hoc, à charge pour le responsable de l'audit interne de s'appuyer sur les conclusions de ce rapport. Dans d'autres cas, et en particulier lors d'une co-traitance, le prestataire produira un livrable intermédiaire qui sera intégré dans un rapport du service d'audit.

Selon la MPA 1210.A1-1 Recours à des prestataires externes

« En cas de recours à un prestataire externe, le responsable de l'audit interne peut, si nécessaire, mentionner les services ainsi fournis dans les documents ou rapports émis au titre de la mission. Le prestataire externe est informé et, le cas échéant, son accord devrait être obtenu avant toute mention de ses services dans ces documents. »

© IFACI

Les livrables attendus à chaque étape de la réalisation de la mission doivent être précisément spécifiés.

Point de vigilance

Le responsable de l'audit interne devrait être particulièrement attentif aux aspects liés à la communication et au suivi des recommandations.

Les étapes à couvrir par le prestataire et les attentes correspondantes doivent donc être spécifiées (livrables attendus, implication du prestataire dans la communication interne, outils, capacité à pondérer des « meilleures pratiques » au regard de la culture interne…).

La nature même du contrat dépendra de l'historique de la relation avec le prestataire et de l'étendue des missions convenues : s'agissant d'une relation établie ou d'un volume important de sous-traitance, la mission pourra s'inscrire dans le cadre d'un contrat cadre annuel, éventuellement complété par avenant.

Il n'existe pas de « contrat type ». La structure proposée ci-dessous n'est qu'une trame à adapter.

Objet du contrat	• Contexte de l'intervention • Périmètre de la mission, définition des objectifs et des livrables attendus • Agréments ou certifications requis du prestataire et profils recherchés
Obligations	• Obligations du service d'audit interne • Obligations du prestataire • Durée de l'intervention • Conditions d'exécution des prestations (par exemple, avec ou sans co-traitance) • Modalités de suivi des travaux
Durée et exécution	• Durée de l'intervention • Conditions d'exécution des prestations (par exemple, avec ou sans co-traitance) • Modalités de suivi des travaux
Méthodologie	• Obligations en matière de documentation des travaux et d'outils • Conformité avec les normes professionnelles et les référentiels internes • Contenu et format des livrables intermédiaires et finaux • Propriété des papiers de travail, rapports et autres documents produits dans le cadre de la mission
Conditions financières	• Prix • Indexation • Révision des prix • Facturation et modalités de paiement • Pénalités et sanctions

© IFACI

Sécurité et confidentialité	• Sécurité et sauvegarde des données • Confidentialité • Archivage
Autres dispositions	• Définition des responsabilités aux différents stades de la mission • Modalités d'exécution, de supervision et de suivi des travaux, intégrant le suivi du temps passé • Respect des engagements contractuels et principes de facturation (mesure du service rendu) • Evaluation de la mission et des compétences du prestataire à la fin de la mission • Définition des limites de responsabilités *(liabilities)*

3.2.2- Clauses spécifiques

Les clauses spécifiques généralement utilisées concernent :

>> La confidentialité

Compte tenu de la nature des diligences réalisées (tests sur les accès, test d'intrusion…) et de la sensibilité des données ou des résultats, la confidentialité des informations doit être assurée.

En signant le contrat qui comporte cette clause, le prestataire s'engage à garder le secret et à sécuriser l'information pendant et après son intervention. Le cas échéant, les membres de l'équipe peuvent également signer une lettre d'engagement de confidentialité.

>> Le transfert de propriété

Dans le cas d'une mission d'audit SI, le transfert de propriété peut concerner par exemple le transfert de scripts ayant servi à la réalisation de requêtes, ou bien le transfert de programmes d'analyse de données utilisés dans le cadre de la mission.

© IFACI

Partie 4

Pilotage de la prestation et de la mission

Une fois le prestataire sélectionné et son intervention cadrée contractuellement et techniquement (cf. 3- Modalités pratiques d'engagement d'un prestataire), les travaux d'audit peuvent démarrer. Il est alors impératif de mettre en œuvre un dispositif de pilotage (cf. 4.1- Cadre de pilotage à mettre en œuvre) et de suivi des travaux réalisés (cf. 4.2- Gestion de la relation avec le prestataire) afin de garantir la réussite des missions.

Bien que ce dispositif s'apparente au « protocole » défini par le responsable de l'audit interne pour contrôler les travaux réalisés par les auditeurs internes, le recours à des prestataires externes entraine des spécificités décrites ci-après (cf. 4.3- Contrôle des travaux réalisés et 4.4- Contrôle de l'efficience du contrat et plans d'actions).

© IFACI

4.1- Cadre de pilotage à mettre en œuvre

Le pilotage d'une prestation externe repose essentiellement sur le contrat (cf. 3.2) qui doit notamment permettre de contrôler deux éléments corrélés : la relation avec le prestataire (la prestation) et la mise en œuvre opérationnelle (la mission). Ce dispositif général de pilotage est schématisé ci-dessous. Sa déclinaison dépendra des choix propres à chaque organisation.
Le responsable de l'audit interne pourra, par exemple, décider de déléguer le suivi opérationnel à un chef de mission interne[29].

Rôle et profil d'un chef de mission interne

Pour faciliter le suivi opérationnel de la mission, le responsable de l'audit interne pourra décider de désigner, dans son service, un chef de mission qui assurera la relation quotidienne avec les prestataires[30].
Ce chef de mission devra avoir :

- un certain niveau de séniorité et d'autorité pour interagir avec l'équipe de prestataires et faciliter la relation avec les audités ;
- une connaissance suffisante des méthodes d'audit interne pour assurer la revue qualité des travaux ;
- une maîtrise des bonnes pratiques en matière de contrôle interne, de gestion des risques et de gouvernance pour le suivi des objectifs de la mission ;
- une aisance en communication lui permettant d'exprimer précisément ses idées, instructions et attentes ;
- des compétences de gestion de projet ;
- des capacités de résolution de problèmes.

Le rôle du chef de mission interne prend une tonalité particulière en cas de co-traitance car il doit assurer l'articulation entre équipe interne et externe. Dans tous les cas, il rend régulièrement compte au responsable de l'audit interne qui est ultimement responsable de la gestion de la relation avec le représentant légal du prestataire et procède rapidement aux arbitrages nécessaires.

Les modalités d'application des éléments du cadre de pilotage pourront varier en fonction de la nature de la mission et du degré d'intégration des prestataires (co-traitance : intégration d'une ressource externe au sein d'une équipe d'auditeurs internes ou sous-traitance : pilotage par le chef de mission d'une équipe de prestataires travaillant de façon autonome). Dans tous les cas, l'équipe de prestataires sera encadrée de manière opérationnelle par un chef d'équipe externe qui rend compte au représentant légal du prestataire tel que défini par le contrat.

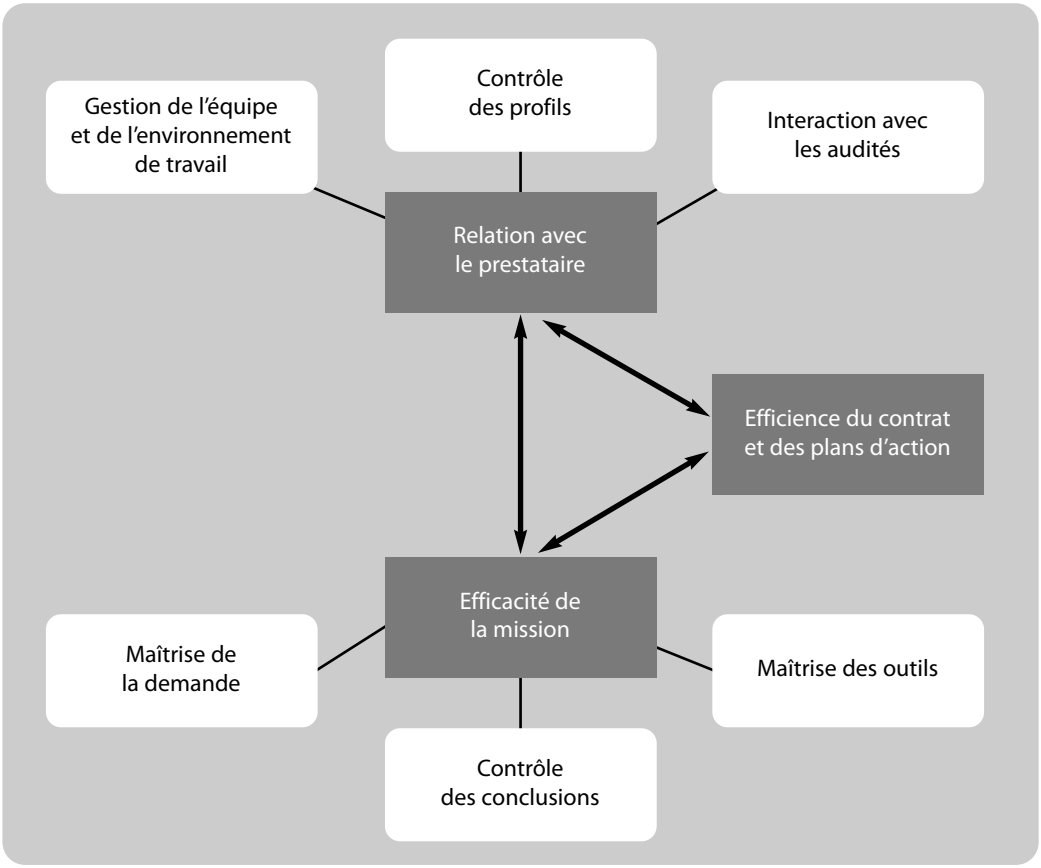
---

[29] *Dans la suite du texte l'expression « chef de mission » sera utilisée pour désigner ce collaborateur interne. Les membre de l'équipe du prestataire par « prestataires » ou « intervenants »*

[30] *Cf. IIA South Africa, White paper : Managing the outsourced internal audit function. P9-10*

© IFACI

Schéma n°3 : Cadre de pilotage de la prestation



Les missions d'audit, plus courtes que des projets pluriannuels, n'offrent pas la même souplesse en matière d'application des clauses contractuelles, voire de révocation d'une ressource. Il est donc impératif de définir avec précision les critères nécessaires pour assurer le succès de la mission (cf. 2.2.2, 3.1.2 et 3.2).

Les exigences identifiées lors de l'appel d'offres, et qui n'auraient pas fait l'objet d'une clause contractuelle, devront néanmoins être prises en compte dans le pilotage de la prestation (cf. 4.2) et de la mission (cf. 4.3). Ce suivi vise à maitriser des risques tant pour le prestataire que pour le service d'audit[31]. Par exemple :

- des risques de conflits du fait de la violation de clauses contractuelles ou de leur imprécision (par exemple en matière de gestion de la confidentialité) ;
- l'augmentation du coût de la prestation (budget temps et financier) ;
- des impacts sur les collaborateurs du service (compétences, motivation, charge de travail...) ;
- des risques d'image vis-à-vis des audités.

[31] *Cf. risques liés à l'infogérance : Global Technology Audit Guide (GTAG) 7 - L'infogérance, 2ème édition / IIA / IFACI, juin 2012*

© IFACI

Bonne pratique

Au démarrage de la mission, il est primordial que le responsable de l'audit (ou son délégataire) explicite aux membres de l'équipe du prestataire :

- les grandes lignes de l'environnement de contrôle de l'organisation ;
- le positionnement du service d'audit ;
- la vision et l'approche d'audit en lien avec la charte validée par les instances de gouvernance ;
- le contexte de la prestation et les principaux attendus.

4.2- Gestion de la relation avec le prestataire

Quelle que soit la nature des travaux, la maitrise de la prestation passe par :

- la qualité des profils en présence (compétences techniques et relationnelles) ;
- l'accès aux ressources (stabilité des intervenants, suppléance éventuelle, logistique) ;
- la gestion de l'interaction avec les audités.

Ces éléments ont un impact sur la conduite de la mission (cf. 4.3) et alimente le retour d'expérience de l'audit interne (cf. 4.4).

4.2.1- Contrôle des profils et des compétences associées

Certains critères déterminants pour la réussite de la mission, identifiés lors de l'appel d'offres (cf. 3.1), peuvent être formalisés dans le contrat (par exemple : le domaine et le niveau d'expertise attendus ou le degré d'indépendance). Les autres éléments du profil (en particulier : la qualité de l'expression orale et écrite, le niveau d'autonomie, la motivation) devraient en plus faire l'objet d'un suivi tout au long de la prestation par le responsable de l'audit interne. Le remplacement d'une ressource étant d'autant plus difficile à faire que la mission est avancée, il est donc préférable d'anticiper autant que possible l'évaluation de ces compétences.

Bonne pratique

Vérifier le profil des personnes effectivement mobilisées par le prestataire.

A partir des prérequis stipulés dans le contrat ou lors de la sélection du prestataire, le responsable de l'audit interne :

- vérifiera les attestations de compétence (audit interne, SI, certifications…) et les antécédents de chaque consultant affecté à la mission ;
- s'entretiendra avec chacun des membres de l'équipe (au-delà de la vérification des qualifications professionnelles et de la gestion des conflits d'intérêt potentiels, jauger la person-

© IFACI

nalité, la capacité à assumer le rôle prévu, à s'intégrer dans l'organisation et à s'adapter à la culture d'entreprise ;

- confirmera l'adéquation du profil et sa disponibilité en lien avec le rôle assigné dans la mission en particulier pour le chef d'équipe externe (séniorité, capacité de supervision de la mission) et pour les travaux d'expertise.

En lien avec les conclusions des évaluations du responsable de l'audit interne, le chef d'équipe externe veille au respect des critères ci-dessus, en particulier le niveau d'autonomie et de motivation de ses collaborateurs. En effet, ces critères ont un impact direct et indirect sur la qualité de la mission et sur la capacité d'intégration des prestataires. Mal maîtrisés, ces paramètres peuvent entraîner une baisse de motivation de l'ensemble de l'équipe, y compris des collaborateurs internes dans le cas de la co-traitance.

En cas d'évolution du périmètre de la mission, le niveau d'expertise et d'indépendance des prestataires externes devra être réévalué. Par exemple, si une nouvelle direction doit être auditée, il est indispensable de s'assurer qu'aucune des missions préalablement réalisées par les intervenants externes ne crée de conflit d'intérêt. De même, si les investigations menées demandent une expertise non identifiée dans le cahier des charges, il est nécessaire de vérifier que les intervenants disposent de cette expertise ou, à défaut, qu'une expertise ponctuelle peut leur être apportée.

4.2.2- Gestion de l'équipe de prestataires et de l'environnement de travail

En cas de recours à une prestation externe pour réaliser une mission d'audit, le prestataire est seul responsable de la gestion de ses ressources. Dans ce contexte, le responsable de l'audit interne doit adresser ses exigences et remarques (règles et pratiques de l'entreprise, spécifications de la mission) au représentant légal du prestataire qui les prendra en compte et déléguera, le cas échéant, leur mise en œuvre au chef d'équipe externe.

Malgré une tension sur la disponibilité des profils les plus spécialisés et les plus techniques, le responsable de l'audit interne doit s'assurer que le remplacement d'une ressource externe n'impactera pas la qualité de la mission et le respect des délais. Le cas échéant, le prestataire sera tenu d'informer le responsable de l'audit interne de toute substitution de ressources envisagée. Ce dernier, vérifie que les termes du contrat ne sont pas remis en cause et que le profil des nouveaux intervenants répond aux critères attendus. Une définition préalable des critères d'éligibilité et de compétences pour chaque rôle facilitera cette vérification.

Selon le contexte de l'intervention, il convient de déterminer si les travaux sont, en tout ou partie, réalisés dans les locaux de l'organisation et de préparer en conséquent l'accès des prestataires aux bureaux (badges d'accès, accompagnement des prestataires par un collaborateur interne…).

© IFACI

Certaines analyses peuvent être réalisées à distance. Néanmoins, les réaliser en interne favorise l'interaction avec les auditeurs et permet de maîtriser des enjeux de sécurité. Surtout lorsqu'il s'agit de travailler sur des applications clés de l'organisation qui nécessiteraient une ouverture de flux sensibles d'un point de vue sécurité.

Dans tous les cas, le responsable de l'audit interne doit s'assurer que l'équipe du prestataire sera pleinement opérationnelle durant la mission d'audit en veillant à leur fournir les accès aux informations et aux ressources informatiques nécessaires. Certaines demandes d'accès ou de ressources (environnements techniques dédiés par exemple) devront être anticipées suffisamment à l'avance auprès du service informatique. En outre, le responsable de l'audit interne fournira au prestataire un environnement de travail (par exemple : support de stockage de données protégé) permettant le respect des clauses de confidentialité telles que défini dans le contrat.

Si les travaux nécessitent l'accès aux locaux d'un sous-traitant, il faudra s'assurer que le contrat établi entre l'organisation et le sous-traitant autorise un tel accès. Le responsable de l'audit interne s'assurera, le cas échéant, de respecter les délais contractuels de mise en œuvre de ces autorisations d'accès.

4.2.3- Maîtrise des interactions entre le prestataire et les audités

La qualité de la relation entre auditeurs et audités est un facteur clé de succès de la mission. Dans le cas du recours à des prestataires externes les principes de cette interaction devront être définis, rappelés au démarrage de la mission et leur application contrôlée tout au long de la prestation.

A titre d'illustration : Règles et forme de l'interaction

- Informer les audités du cadre global d'intervention des prestataires externes (dans la lettre de mission ou en réunion d'ouverture), le cas échéant, le rappeler à chaque étape (phase de test, restitution).
- Veiller à une fréquence de sollicitation raisonnable des audités.
- Informer systématiquement et formellement le responsable de l'audit interne de tout échange avec les audités.
- Suivre les délais de réponse des audités et, le cas échéant, intervenir pour appuyer la demande du prestataire externe.
- Etre attentif à l'adéquation du niveau de discours en fonction de l'interlocuteur.
- Prévoir la présence d'un auditeur interne lors des échanges clés avec les audités.
- Toujours préparer les échanges (ordre du jour, type d'informations communiquées et prise de position du prestataire externe) avant sollicitation des audités.
- Etre systématiquement destinataire des comptes rendus d'entretien.

© IFACI

4.3- Contrôle des travaux réalisés

La qualité de la relation avec le prestataire externe (cf. 4.2) et l'implication directe sur le terrain de ressources internes (chef de mission) garantissent la pertinence et la qualité des travaux effectués. Le chef de mission devra en particulier s'assurer que la méthodologie et les outils mobilisés par les prestataires sont conformes aux termes du contrat et adaptés aux objectifs de la mission. Il veillera également à la robustesse des analyses et des conclusions formulées par les prestataires.

4.3.1- Maîtrise de la méthodologie

Le prestataire externe se doit de se conformer à la méthodologie du service d'audit interne et de respecter les étapes clés préalablement définies et planifiées (note de cadrage, programme de travail, entretiens, tests, réunions de validation, rapport final, le cas échéant, le suivi des actions correctives).

Cette mise en conformité est facilitée dans le cas d'une co-traitance puisque le prestataire est « embarqué » dans l'équipe interne. Le responsable de l'audit interne devra accorder une vigilance particulière au respect de la méthodologie dans le cas d'une sous-traitance partielle ou totale afin de maîtriser l'articulation avec d'autres volets de la mission ou d'autres activités du service d'audit interne. La référence au Cadre de référence international des pratiques professionnelles d'audit interne facilitera la convergence des approches.

Il convient également d'être attentif aux méthodologies spécifiques à l'audit informatique employées par les prestataires externes.
Le service d'audit interne devrait disposer a minima de connaissances élémentaires[32] des référentiels SI (COBIT, ISO, ITIL, e-SCM, GTAG…) à travers des formations régulières. Ces connaissances permettront de discuter avec le prestataire de certains objectifs d'audit informatique (gouvernance du SI, projet informatique, externalisation…).

En revanche, pour des audits informatiques plus techniques, comme les tests d'intrusion, les revues de codes, les analyses de performance ou les revues de sécurité physique, l'absence d'experts au sein du service d'audit interne rendrait plus difficile l'appréciation du bien-fondé de la méthodologie employée. Le responsable de l'audit interne pourra néanmoins examiner les arguments avancés par le prestataire en vérifiant la réputation des méthodologies utilisées ou en contactant des organisations les ayant déjà éprouvées. Il peut également demander conseil à des experts internes (DSI, RSSI, gestion des risques, contrôle interne…). Sous réserve de veiller à l'objectivité de ces avis, le responsable de l'audit interne pourra obtenir un accord préalable sur la méthodologie du prestataire externe et pourra également solliciter ces référents internes pour vérifier la pertinence des résultats (cf. 4.3.3).

[32] *Cf. CRIPP 2014 : Norme 1210.A3 Niveau de connaissance des principaux risques et contrôles relatifs aux technologies de l'information*

© IFACI

4.3.2- Maîtrise et déploiement des outils

Les prestataires externes devront maîtriser et utiliser les outils informatiques nécessaires à la réalisation de la mission. Ils pourront être formés aux environnements spécifiques utilisés par l'audit interne au cours d'une étape d'intégration (cf. 4.2.2).

Lorsque les prestataires disposent d'outils spécifiques pour la réalisation de tests techniques (tests d'intrusion, outils d'injections SQL pour mesurer la robustesse de code d'une page web, outils d'évaluation des vulnérabilités de systèmes, analyse des accès utilisateur et de la séparation des tâches…), leurs modalités d'utilisation et les protocoles de tests doivent être discutés avec le RSSI et validés avec la DSI pour maîtriser les risques de perturbation de l'environnement de production informatique.

L'extraction de données peut impliquer un temps de mise en œuvre assez long qui doit donc être anticipé. Une formation aux outils d'extraction de données utilisés par le prestataire peut être envisagée pour optimiser le temps de préparation des scripts et des fichiers. A terme, un transfert de compétences pourra également être envisagé pour les outils ne nécessitant pas une forte technicité. En effet, l'industrialisation de certains tests permettra de les faire tourner périodiquement en support des audits classiques.

4.3.3- Contrôles des analyses et des conclusions du prestataire

La supervision des travaux du prestataire doit être assurée par un chef de mission interne ayant un niveau de séniorité suffisant.

Bonne pratique

Conformément aux bonnes pratiques professionnelles[33], la supervision vise à s'assurer d'une bonne couverture du périmètre et des objectifs de la mission définis dans le contrat et la lettre de mission. Le responsable de l'audit interne aura donc pris le soin d'aborder précisément avec le prestataire les éléments suivants :

- les livrables et les échéances ;
- les points particuliers devant figurer dans les rapports remis au titre de la mission ;
- l'accès aux documents, aux personnes et aux biens concernés ;
- les hypothèses et les procédures à utiliser ;
- la propriété et la conservation des documents de travail ;
- la conformité aux Normes internationales d'audit interne.

Le chef de mission devra s'assurer tout au long de l'intervention des prestataires externes que le juste niveau d'information leur est communiqué, tout en respectant et en faisant respecter la confidentialité.

[33] *Cf. CRIPP 2014 : MPA 1210.A1-1*

© IFACI

Les modalités de suivi peuvent revêtir plusieurs formes : compte rendus écrits périodiques des travaux réalisés, réunions régulières de suivi pour la présentation de l'avancement et des analyses envisagées, etc. Ces échanges devront être tracés pour faciliter le pilotage de la mission et le suivi contractuel de la prestation (cf. 4.4). La nature du suivi dépendra, entre autres, des modalités de sous-traitance, du nombre d'intervenants externes, du nombre de sites concernés, de la durée de la mission.

Une attention particulière doit être portée sur la bonne compréhension, par les prestataires externes, des travaux sous leur responsabilité. Pour cela, il convient de les impliquer dès la phase de cadrage des travaux. A défaut, le chef de mission devra consacrer le temps nécessaire à la présentation des axes d'analyse et s'assurer que les prestataires ont bien saisi les enjeux de la mission. Par la suite, les programmes de travail et les plans de test proposés par les prestataires permettront d'objectiver la prise en compte effective de ces enjeux.

Même dans le cas d'une sous-traitance totale, le responsable de l'audit interne devra contrôler la profondeur et l'exhaustivité des analyses réalisées en vue de soutenir les constats auprès des audités et d'assurer le suivi des actions correctives. Il est donc nécessaire que le prestataire documente rigoureusement ses hypothèses de travail et les tests utilisés pour aboutir à ses conclusions. Même dans le cas de missions plus techniques pour lesquelles l'audit interne ne possède pas d'expertise en interne[34], le chef de mission doit être capable de comprendre et de challenger le prestataire externe.

Le suivi rapproché des travaux réalisés ne dispense pas le chef de mission d'un contrôle des conclusions d'audit, ainsi que des recommandations qui en découlent. Parmi les éléments structurants[35] à vérifier, citons :

- la structuration du raisonnement. Le chef de mission devra vérifier que la démonstration est compréhensible, factuelle, et documentée. La qualité de l'argumentation dépendra fortement de l'expertise « audit » de l'intervenant et de son expérience ;
- la qualité des pistes d'audit. Ces dernières doivent être suffisantes, fiables, pertinentes et utiles[36] au regard des objectifs de la mission. Par exemple, les scénarios de tests devraient être régulièrement contrôlés par le chef de mission. En revanche, les preuves d'audit ne sont pas nécessairement communiquées et donc contrôlées préalablement à la livraison des conclusions. Une vérification par échantillonnage de ces pistes d'audit permettra d'optimiser le temps consacré à la supervision ;
- l'exploitation des tests réalisés. Bien qu'il soit nécessaire de contrôler régulièrement la robustesse des tests, leur intérêt dans une démonstration ne peut être constaté qu'une fois les analyses terminées. Le chef de mission doit notamment s'assurer qu'aucun résultat n'est généralisé à tort et que l'exploitation qui en est faite permet effectivement d'alimenter l'argumentation. Ici encore l'expertise « audit » de l'intervenant externe sera déterminante ;

[34] *Cf. CRIPP 2014 : Norme 1210.A3 Niveau de connaissance des principaux risques et contrôles relatifs aux technologies de l'information*

[35] *Cf. CRIPP 2014 : Normes 2310 Identification des informations, Norme 2420 Qualité de la communication*

[36] *Cf. CRIPP 2014 : Norme 2310 Identification des informations*

© IFACI

- la pertinence des conclusions et leur contextualisation. Ces aspects sont particulièrement sensibles dans le cas du recours à des prestations externes et permettent d'éviter que les travaux ne soient trop génériques ou inexploitables par l'organisation ;
- le contrôle qualité prévu dans le cadre des procédures d'auto-évaluation du service d'audit[37] ;
- le format des livrables conformément au cadre contractuel.

Le contrôle des analyses et des conclusions du prestataire s'appuie sur le cadre contractuel qui précise généralement l'exhaustivité du périmètre à analyser et détermine la profondeur de test attendue, les indicateurs de réalisation et leurs modalités de suivi.

Le cadre contractuel est en général plus précis dans le cas de missions nécessitant une expertise ou dans le cas d'une sous-traitance. Par exemple, les scénarios des tests d'intrusion peuvent détailler les risques à couvrir, le périmètre visé (applications, types d'accès, etc.), les conditions de réalisation de ces tests (audit de type boite noire, boite blanche, avec ou sans habilitations, en production ou non, etc.) ainsi que les indicateurs cibles de couverture ou d'avancement des tests (cf. 4.4).

A défaut d'être définies dans le cadre contractuel, ces exigences devront être précisées dès le début de la mission par le responsable de l'audit interne.

Malgré la supervision, et à la suite du contrôle des livrables produits, il peut être nécessaire de demander aux intervenants externes des compléments d'analyse. Pour maîtriser ces aléas et éviter de se retrouver à corriger seuls les éventuelles défaillances, il est recommandé de prévoir suffisamment de temps entre la livraison des conclusions et la fin de la prestation. Sachant que l'élaboration des conclusions passe par plusieurs étapes : formalisation des constats après la phase terrain, réunion de clôture avec les audités, intégration dans le rapport, formulation définitive des recommandations, validation des plans d'action avec les audités ; il convient donc de déterminer en amont l'implication ou non du prestataire pour chacune de ces étapes.

4.4- Contrôle de l'efficience du contrat et plans d'actions

Le pilotage de la relation avec le prestataire et la supervision des travaux sont facilités par le suivi d'indicateurs clés notamment budgétaires (cf. schéma en 4.1). L'analyse globale du respect du contrat et de sa plus-value devrait systématiquement être effectuée pour conforter les orientations stratégiques du service d'audit interne (cf. 2.1) et son amélioration continue.

[37] *Cf. CRIPP 2014 : Norme 1300 Programme d'assurance et d'amélioration qualité*

© IFACI

Bonne pratique

Tous les indicateurs de suivi n'étant pas précisément définis dans le cadre contractuel, il convient, dès le démarrage de la mission, de présenter au prestataire les critères qui seront utilisés. Leurs modalités de mesure, leurs traitement (ou les pénalités éventuelles) devront également être définis d'un commun accord.

Le responsable de l'audit interne peut décider de déléguer ce suivi à un collaborateur autre que le chef de mission chargé de la supervision des travaux.

Le cas échéant, pour les missions complexes, de longue durée, ou réalisées en parallèle par le même prestataire, un comité de pilotage pourra être instauré. Il est alors composé des parties prenantes internes concernées (responsable de l'audit interne, chef(s) de mission, le cas échéant, le chargé du suivi de performance et/ou le responsable méthode, le référent SI ...) ainsi que les représentants du prestataire (représentant légal, chef de projet externe, le cas échéant, le commercial). En tout état de cause, le responsable de l'audit interne assume *in fine* la responsabilité des choix opérés.

Généralement, le suivi est réalisé au travers de réunions périodiques permettant d'échanger sur :

- l'évolution des indicateurs de performance du prestataire (coût, qualité, délai, transfert de compétence…) ;
- les engagements pris par le responsable de l'audit interne pour faciliter la réalisation de la mission (transmission correcte des informations nécessaires, disponibilité et réactivité du chef de mission, préparation de l'environnement de travail et des interactions avec les audités…).

Le contrat constitue une première ligne de défense pour la gestion d'éventuels écarts. Pour cela, il doit avoir été préparé avec soin, être suffisamment précis et adapté à la mission (cf. 3.2). Pour autant, compte tenu de la durée relativement courte des missions d'audit et de la rareté de certaines ressources, il est préférable d'établir un dialogue permanent et constructif avec le prestataire. Souvent, le coût de remplacement du prestataire en cours de mission ne permet pas, en pratique, d'envisager une rupture du contrat. De même, il est préférable d'éviter d'en venir à l'application de clauses de pénalités ou au contentieux qui ne résoudraient en rien les problèmes de qualité et de délais souvent critiques pour la réalisation d'un plan d'audit.

Les réunions de suivi doivent permettre de mesurer la performance actuelle par rapport à la cible et d'en tirer les conséquences (revue des indicateurs cibles, modulation de la volumétrie de la prestation, substitution d'intervenants, ressources supplémentaires, renégociation d'honoraires...).

Point de vigilance

Certains travaux d'audit informatique peuvent nécessiter des coûts additionnels externes ou internes qu'il convient de prévoir (cf. partie 2) et de suivre avec précision pour ne pas fausser l'évaluation de l'efficience de la prestation.

© IFACI

Les bonnes pratiques de résolution de problèmes aideront le responsable de l'audit interne dans l'élaboration de plans d'action efficients.

1- s'accorder avec le prestataire sur la nature du problème ;
2- évaluer la cause du problème (manque d'information, incompréhension, manque de compétence, manque de motivation…) ;
3- présenter et discuter les scénarios de résolution et leurs limites (par exemple, un problème d'information peut être facilement résolu par la mise à disposition des informations ad hoc. En revanche, le recours à une ressource rare peut induire des problématiques de coûts ou de disponibilité sur le créneau prévu) ;
4- recadrer et procéder à un suivi plus rapproché ou, le cas échéant, fixer de nouveaux objectifs et informer le représentant légal du prestataire.

Point de vigilance

Lors que les solutions envisagées sortent du cadre contractuel initial, il est conseillé de les formaliser à travers un avenant.

Il est indispensable de garder des traces écrites des relances et ajustements adressés aux prestataires pour éventuellement faire jouer des pénalités ou clauses prévues au contrat.

L'analyse et le traitement des problèmes doivent être pris en compte pour alimenter le retour d'expérience du service d'audit interne et constituer une source d'apprentissage pour les futurs recours à des prestataires externes. Il est également recommandé d'informer la direction des achats pour le suivi des prestataires dans la durée et faire en sorte que les éventuels problèmes de qualité constatés lors de la prestation soient connus lors des appels d'offre ultérieurs.

A l'issue de la prestation, le responsable de l'audit devrait procéder à un débriefing interne pour évaluer le retour sur investissement du contrat : temps passé en pilotage, qualité du rendu, impact sur la motivation des collaborateurs internes, leur moral, leurs compétences internes ou l'image du service. Ce bilan peut servir pour la comparaison de différents prestataires ou la révision des orientations stratégiques de recours à des prestations externes, y compris, le cas échéant, en termes de réversibilité (cf. 2.1).

© IFACI

ANNEXES

© IFACI

Annexe 1 : Exemple de missions d'audit des SI

Ce tableau a été réalisé à partir des pratiques des membres de l'unité de recherche. Les activités d'audit des SI recommandées par la Fondation de la recherche de l'IIA à l'issue du CBOK 2015 ont également été prises en compte (cf. CBOK : Navigating technology's Top 10 risks / IIARF, octobre 2015).

Catégories de mission	Sous famille	Exemples de mission
Gouvernance des SI	• Planification du SI et intégration dans le plan stratégique de l'entreprise • Urbanisme et architecture du SI de l'entreprise au service des enjeux stratégiques • Gestion du portefeuille de projets orienté création de valeur pour les métiers • Management des risques SI en fonction de leurs impacts métiers • Alignement de la fonction informatique par rapport aux processus métiers • Maîtrise de la réalisation des projets en fonction des enjeux métiers • Fourniture de services informatiques conformes aux attentes clients • Pilotage des services externalisés • Contrôle de gestion informatique favorisant la transparence • Gestion prospective des compétences informatique • Gestion et mesure de la performance du SI	• Evaluation du degré d'adaptation des ressources organisationnelles (structures), humaines et financières consacrées par l'organisation à l'informatique ; • Revue du fonctionnement de la comitologie (implication des utilisateurs, portage au niveau hiérarchique adéquat) associée au pilotage des SI • Evaluation des politiques et procédures en place et de leur application effective, en particulier pour les projets hors budget ou hors délais ; • Evaluation du schéma directeur ; • Revue de l'organisation, des responsabilités et des modes de pilotage de la fonction SI ; • Revue du pilotage de la performance ; • Evaluation de l'adéquation fonctionnelle, de l'urbanisation et du patrimoine applicatif ; • Revue des compétences critiques ou clés et des qualifications des collaborateurs ; • Revue des coûts IS/IT ; • Analyse post-mortem.
	• Audit des infrastructures (système d'exploitation, base de données, réseaux, environnement physique, cloud…)	• évaluation de la conformité à la politique et aux procédures réseau.

© IFACI

Catégories de mission	Sous famille	Exemples de mission
Gouvernance des SI *(suite)*	• Prestations informatiques externalisées	• Revue des données et informations échangées dans le cadre de la prestation (maîtrise de la confidentialité et de la sécurité des données) ; • Identification des ressources informatiques matérielles concernées ; • Revue des aspects SI dans le cadre de la relation contractuelle ; • Revue des contrats des principaux prestataires (montant mais également domaine à risque) ; • Revue des modalités de définition des livrables ; • Evaluation des critères du service fait ; • Revue des contrôles réalisés par le prestataire (y compris les rapports SSAE (Statement on Standards for Attestation Engagements) 16.
Support à la revue de processus opérationnels et fonctionnels	• Analyse de données • Contrôle en continu	• Evaluation de la contribution des outils informatiques à l'efficacité et à l'effectivité du dispositif de contrôle interne du processus.
	• Contrôles applicatifs	• Revue de la qualité des données.
	• Régularité / conformité (y compris forensic, cybercriminalité)	• Revue de la conformité réglementaire (CNIL) ; • Conformité des traitements automatiques réalisés par ces ressources au corpus normatif applicable ; • Contrôle de la non-utilisation à des fins frauduleuses de ces ressources ; • Evaluation du respect des règles de confidentialité.

© IFACI

Catégories de mission	Sous famille	Exemples de mission
Contrôles généraux informatiques (relatifs à des applications ou à des infrastructures SI)	• Projets (développement, gestion des changements)	• Adaptation des infrastructures et de l'assistance SI aux besoins du processus ; • Evaluation de l'alignement avec les priorités stratégiques de l'organisation et les besoins métiers ; • Revue de préparation au déploiement ; • Revue post implémentation ; • Revue de l'appropriation par les utilisateurs ; • Revue de la mise en œuvre des bonnes pratiques de gestion de projet (planification, suivi budgétaire, conduite du changement, etc.) ; • Revue de l'adéquation des applications aux besoins ; • Revue de la performance et de la rentabilité des applications ; • Revue de la pérennité et de l'évolutivité de l'application ; • Evaluation de conformité des licences logiciels (contract compliance).
	• Accès logiques et physiques	• Evaluation de la cohérence de la sécurité physique et logique des données, applications et infrastructures avec l'analyse des risques du processus ; • Revue de l'attribution et du suivi des accès à privilèges (exemple administrateurs du système).
	• Production/exploitation (sauvegarde/restauration ; monitoring ; gestion des configurations ; gestion des incidents)	• Revue de configuration ; • Revue d'architecture technique ; • Mission d'audit d'un centre de traitement des données ; • Audit post-incident (utilisation et adéquation des procédures ou outils de gestion des incidents, mobilisation des ressources appropriées, leçons tirées…).

© IFACI

Catégories de mission	Sous famille	Exemples de mission
Contrôles généraux informatiques (relatifs à des applications ou à des infrastructures SI) *(suite)*	• Support utilisateurs	• Revue de la fiabilité du support utilisateurs ; • Revue de la performance et de l'efficacité du support utilisateurs.
	• Plan de secours	• Revue de l'alignement des plans de secours avec les besoins de continuité métiers ; • Revue de la mise en œuvre et de l'efficacité des plans de secours.
	• Sécurité (gouvernance de la sécurité ; cybersécurité …)	• Revue de la politique de sécurité ; • Test de pénétration ; • Revue du contrôle des accès ou des exercices de simulation (exécution et analyse effectives) ; • Test de vulnérabilité et revue de configuration ; • Revue d'architecture technique ; • Adéquation avec la politique de gestion de crise ; • Evaluation de la conformité et de l'efficacité des procédures de protection des données notamment les données personnelles.

© IFACI

MAÎTRISER LE RECOURS À DES PRESTATIONS EXTERNES D'AUDIT

Annexe 2 : Tableau de suivi

AVERTISSMENT: Cette grille est donnée à titre d'exemple et devra être adaptée en fonction des objectifs d'audit et et selon le type de prestations (co-traitance, sous-traitance...)

Intitulé de la mission : sécurité logique et physique

Dernière mise à jour : XX février XXXX

Objectifs d'audit*	Objectifs de contrôle	Acteur (SAI, prestataire)		Début de la phase de planification	Début de la phase de réalisation	Fin de la phase de réalisation	Envoi du projet de rapport au chef de mission	Envoi du projet aux audités	Réponses des audités	Rapport final	Remarques
Efficacité de l'organisation de la DSI		Prestataire	**Prévision –>**	sem. du 17/07	4 août	24 août	31 août	7 sept.	21 Sept.	15 déc.	
			Réalisé –>	✓	✓	✓	✓	✓	✓	N/A	Conclusions et recommandations finalisées à intégrer au rapport global de la mission
Evaluation de la formalisation et mise en œuvre de la politique de sécurité et des règles de sécurité (y compris sensibilisation)		SAI	**Prévision –>**	sem. du 25/07	19 sept.	20 oct.	10 nov.	20 nov.	5 déc.	19 déc.	
			Réalisé –>	✓	✓	Voir les remarques					Plan d'action modifié à partir des réunions tenues la semaine 02/10. Le chef de mission devra completer les définitions des objectifs de contrôle avant fin-septembre
Conformité des systèmes avec la politique de sécurité		Prestataire	**Prévision –>**	sem. du 12/07	12 sept.	3 oct.	7 oct.	14 oct.	28 oct.	15 déc.	
			Réalisé –>	✓	✓	14 oct.	21 oct.	18 nov.	30 déc.		En attente d'approbation
Efficacité et adéquation du processus de gestion des risques liés à la sécurité logique et aux accès		SAI / Prestataire	**Prévision –>**	sem. du 25/07	15 août	26 août	16 sept.	23 sept.	13 oct.	19 déc.	
			Réalisé –>	✓	✓	✓	25 sept.	28 sept.	14 oct.	✓	Conclusions et recommandations finalisées
Vérification de la sécurité des accès aux locaux		Prestataire	**Prévision –>**	sem. du 25/08	12 sept.	21 sept.	28 sept.	5 oct.	15 oct.	15 déc.	
			Réalisé –>	✓	✓	✓	✓	✓	✓	N/A	Conclusions et recommandations finalisées à intégrer au rapport global de la mission
Evaluation des procédures de gestion des accès utilisateurs		SAI	**Prévision –>**	sem. du 1/08	15 août	30 sept.	7 oct.	14 oct.	28 oct.	15 déc.	
			Réalisé –>	✓	✓	✓					
Evaluation de la sécurité des accès aux programmes et aux données	L'identification des utilisateurs est-elle exhaustive ?	SAI	**Prévision –>**	sem. du 26/09	17 oct.	25 oct.	1 nov.	4 nov.	18 nov.	15 déc.	
			Réalisé –>	✓	24 oct.	22 nov.	1 déc.	19 déc.	7 janv.	10 janv.	Rapport provisoire en attente de réponse du management
	L'authentification de tous les accès aux programmes et aux données est-elle effective ?	Prestataire	**Prévision –>**	sem. du 3/10	7 nov.	9 déc.	14 déc.	16 déc.	27 déc.	30 déc.	
			Réalisé –>	✓	✓	✓	✓	✓	✓	✓	Rapport révisé
	Les procédures de gestion des comptes utilisateurs sont-elles appliquées ?	SAI	**Prévision –>**	sem. du 10/10	4 nov.	28 nov.	8 déc.	12 déc.	22 déc.	30 déc.	
			Réalisé –>	15 oct.	✓	14 nov.	28 nov.	3 déc.	15 déc.	✓	Référentiel d'audit finalisé
	Le système de revue périodiques des comptes et des accès fonctionne-t-il ? Est-il efficace ?	Prestataire	**Prévision –>**	sem. du 7/11	12 déc.	13 janv.	2 fév.	12 fév.	2 mars	30 mars	Objectif de contrôle annulé, l'accent sera mis sur l'examen de la mise en œuvre des comptes utilisateurs et des comptes privilèges
			Réalisé –>	✓							
	Le principe de séparation des tâches est-il respecté ?	SAI / Prestataire	**Prévision –>**	sem. du 14/11	19 déc.	20 janv.	9 fév.	16 fév.	2 mars	30 mars	
			Réalisé –>	✓	✓	31 janv.					Phase de réalisation à terminer impérativement avant le 27/01

** Rédigé à partir du Guide opérationnel d'application du cadre de référence AMF relatif au contrôle interne "Le contrôle interne du système d'information des organisations" / CIGREF / IFACI, 2009 ** Les dates sont fictives*

ANNEXE

© IFACI

© IFACI

MAÎTRISER LE RECOURS À DES PRESTATIONS EXTERNES D'AUDIT

ANNEXE

Objectifs d'audit*	Objectifs de contrôle	Acteur (SAI, prestataire)		Début de la phase de planification	Début de la phase de réalisation	Fin de la phase de réalisation	Envoi du projet de rapport au chef de mission	Envoi du projet aux audités	Réponses des audités	Rapport final	Remarques
Evaluation de la sécurité des accès aux programmes et aux données *(suite)*	La gestion des comptes privilégiés est-elle efficace ?	Prestataire	**Prévision –>**	sem. du 14/11	19 déc.	20 janv.	9 fév.	16 fév.	2 mars	30 mars	
			Réalisé –>	✓	✓	31 janv.					Phase de réalisation à terminer impérativement avant le 27/01
	La séparation des infrastructures (développement, test, exploitation) est-elle effective ?	Prestataire	**Prévision –>**	sem. du 14/11	19 déc.	20 janv.	9 fév.	16 fév.	2 mars	30 mars	
			Réalisé –>	✓	✓	31 janv.					Phase de réalisation à terminer impérativement avant le 27/01
	Les vulnérabilités techniques sont-elles maîtrisées ?	Prestataire	**Prévision –>**	sem. du 14/11	19 déc.	20 janv.	9 fév.	16 fév.	2 mars	30 mars	
			Réalisé –>	✓	✓	31 janv.					Phase de réalisation à terminer impérativement avant le 27/01
	Les accès aux salles informatiques sont-ils sécurisés ?	Prestataire	**Prévision –>**	sem. du 14/11	19 déc.	20 janv.	9 fév.	16 fév.	2 mars	30 mars	
			Réalisé –>	✓	✓	31 janv.					Phase de réalisation à terminer impérativement avant le 27/01
	Les opérations d'exploitation et de gestion des changements sont-elles correctement documentées ?	Prestataire	**Prévision –>**	sem. du 14/11	19 déc.	20 janv.	9 fév.	16 fév.	2 mars	30 mars	
			Réalisé –>	✓	✓	31 janv.					Phase de réalisation à terminer impérativement avant le 27/01
	La propagation de code malveillants serait-elle maîtrisée ?	Prestataire	**Prévision –>**	sem. du 14/11	19 déc.	20 janv.	9 fév.	16 fév.	2 mars	30 mars	
			Réalisé –>	✓	✓	31 janv.					Phase de réalisation à terminer impérativement avant le 27/01
	La confidentialité (y compris mise aux rebus de matériel) est-elle assurée ?	SAI / Prestataire	**Prévision –>**	sem. du 14/11	19 déc.	20 janv.	9 fév.	16 fév.	2 mars	30 mars	
			Réalisé –>	✓	✓	31 janv.					Phase de réalisation à terminer impérativement avant le 27/01
	Les échanges d'informations en interne et avec l'extérieur sont-ils sécurisés	Prestataire	**Prévision –>**	sem. du 1/12	1 déc.	22 déc.	N/A	N/A	N/A	N/A	
			Réalisé –>	✓	✓	✓					
	L'identification d'activités non autorisées est-elle efficace ?	Prestataire	**Prévision –>**	sem. du 1/12	1 déc.	22 déc.	N/A	N/A	N/A	N/A	
			Réalisé –>	✓	✓	✓					
	Les accès non autorisés au réseau et aux applications sensibles sont-ils maîtrisés ?	SAI / Prestataire	**Prévision –>**	sem. du 14/11	19 déc.	20 janv.	9 fév.	16 fév.	2 mars	30 mars	
			Réalisé –>	✓	✓	31 janv.					
Efficacité et efficience de la surveillance des accès logiques		Prestataire	**Prévision –>**	6 fév.	20 mars	à déterminer	à déterminer	à déterminer	à déterminer	à déterminer	Besoin de préciser les dates
			Réalisé –>								
Sécurité réseau		Prestataire	**Prévision –>**	sem. du 5/12	20 fév.	à déterminer	à déterminer	à déterminer	à déterminer	à déterminer	Réunion d'ouverture prévue le 20/02
			Réalisé –>								
Vérification de la séparation des infrastructures		Prestataire	**Prévision –>**	sem. du 5/12	à déterminer	à déterminer	à déterminer	à déterminer	à déterminer	à déterminer	
			Réalisé –>	✓							Programme de travail en cours d'élaboration

** Rédigé à partir du Guide opérationnel d'application du cadre de référence AMF relatif au contrôle interne "Le contrôle interne du système d'information des organisations" / CIGREF / IFACI, 2009 ** Les dates sont fictives*

ANNEXE

© IFACI

© IFACI

MAÎTRISER LE RECOURS À DES PRESTATIONS EXTERNES D'AUDIT

ANNEXE

Objectifs d'audit*	Intitulé de la mission : sécurité logique et physique	Acteur (SAI, prestataire)		Début de la phase de planification	Début de la phase de réalisation	Fin de la phase de réalisation	Envoi du projet de rapport au chef de mission	Envoi du projet aux audités	Réponses des audités	Rapport final	Remarques
Evaluation du processus de gestion des failles de sécurité		Prestataire	**Prévision –>**	30 janv.	20 fév.	à déterminer	à déterminer	à déterminer	à déterminer	à déterminer	
			Réalisé –>								
Maîtrise des services rendus par les prestataires externes		SAI	**Prévision –>**	sem. du 9/01	sem. du 16/01	17 mars	à déterminer	à déterminer	à déterminer	à déterminer	
			Réalisé –>								
Evaluation du processus de gestion des certificats		Prestataire	**Prévision –>**	sem. du 24/01	7 fév.	à déterminer	à déterminer	à déterminer	à déterminer	à déterminer	
			Réalisé –>								
Efficacité de la gestion des incidents		Prestataire	**Prévision –>**	sem. du 31/01	14 fév.	à déterminer	à déterminer	à déterminer	à déterminer	à déterminer	
			Réalisé –>								
Robustesse du dispositif de protection		Prestataire	**Prévision –>**	sem. du 24/01	21 fév.	à déterminer	à déterminer	à déterminer	à déterminer	à déterminer	
			Réalisé –>								

ANNEXE

© IFACI

© IFACI

MAÎTRISER LE RECOURS À DES PRESTATIONS EXTERNES D'AUDIT

ANNEXE

Eléments connexes de suivi de la mission

Intitulé de la mission		Etape 1	Etape 2	Etape 3	...	% réalisation		Remarques
Méthodologie	Prévision –>	1 juin	11 juil.	30 sept.				
	Réalisé –>	✓	✓			75 %		2ème version à discuter avant mi-juillet
Outils	Prévision –>	sem. du 29/08	7 sept.					
	Réalisé –>	✓	✓					Préciser la documentation de la piste d'audit
Formation	Prévision –>	15 nov.	5 déc.	13 janv.				
	Réalisé –>	✓	✓	✓		100 %		
Déplacements	Prévision –>	21 nov.	6 janv.	13 janv.				
	Réalisé –>	✓	✓	✓		95 %		
Coût de la prestation	Prévision –>	19 janv.	23 janv.	3 fév.				
	Réalisé –>							
Critère 6	Prévision –>							
	Réalisé –>							
Critère 7	Prévision –>							
	Réalisé –>							
Critère 8	Prévision –>							
	Réalisé –>							
Critère 9	Prévision –>							
	Réalisé –>							
Critère 10	Prévision –>							
	Réalisé –>							

ANNEXE

© IFACI

© IFACI

Annexe 3 : Exemple de grille d'évaluation de fin de mission à adapter notamment en fonction du type de prestation (co-traitance ou pas)

Société prestataire : .....

Intitulé de la mission : .....

Intervenant 1 : .....

Intervenant 2 : .....

Intervenant 3 : .....

Evaluateur : .....

Date : JJ/MM/AAAA – JJ/MM/AAAA

	Evaluation (notre de 1 à 4)	Commentaires
1. Evaluation globale de la valeur ajoutée de la prestation		
▶ **Valeur ajoutée pour les métiers** (amélioration de l'identification des risques, moyens de maîtrise contribuant à la performance…)		
▶ **Qualité des constats** (critères d'évaluation explicites, piste d'audit, archivage du dossier d'audit…)		
▶ **Qualité des recommandations** (liens avec les constats, adaptées au contexte...)		
▶ **Valeur ajoutée pour le service d'audit** (délai, périmètre élargie, méthodologie, transfert de compétences…)		
▶ ……..		
Commentaires		
2. Maîtrise de la demande		
▶ **Ecarts par rapport aux objectifs initiaux** (coût, délai, couverture…)		
▶ **Préparation de la mission** (Prise en compte du contexte technique et métier, cartographie des risques…)		
▶ **Objectifs d'audit cohérents avec la demande**		
▶ **Organisation des travaux sur les différents sites**		
▶ **Prise en compte de la méthodologie du service d'audit** (documentation des tests, format des livrables…)		
▶ ……..		
Commentaires		

© IFACI

	Evaluation (notre de 1 à 4)	Commentaires
3. Profils et outils		
▶ **Profils correspondant effectivement à l'offre de service** (séniorité, compétence, disponibilité…)		
▶ **Expertise SI** (référentiels, outils utilisés…)		
▶ **Compréhension des principes et des normes d'audit interne**		
▶ **Capacité à comprendre les points de vue des autres**		
▶ **Force de propositions**		
▶ ……..		
Commentaires		
4. Communication et interactions		
▶ **Minimisation de la perturbation des audités**		
▶ **Réunion d'ouverture** (planification, clarté…)		
▶ **Interactions avec les principales parties prenantes de la mission** (Canaux de communication appropriés , diplomatie…)		
▶ **Relations avec l'équipe d'audit interne**		
▶ **Communication en temps opportun des problèmes et solutions**		
▶ **Réunion de clôture** (présentation factuelle, constructive…)		
▶ ……..		
Commentaires		
5. Autres commentaires, botamment de la part des audités :		

4 – Au-delà des attentes

3 – Au niveau des attentes

2 – Quelques insuffisances

1 – En-deça des attentes

ANNEXE

© IFACI

BIBLIOGRAPHIE

- Cadre de Référence International des Pratiques Professionnelles de l'audit interne / IIA, IFACI, 2014
  - Global Technology Audit Guide (GTAG®) 3 « Audit continu : Coordonner l'audit et le contrôle en continu pour fournir une assurance continue» / IIA, IFACI, 2ème édition, mai 2015
  - Guide Pratique : « Définir un processus de gestion des compétences » / IIA, IFACI, Avril 2015
  - Global Technology Audit Guide (GTAG®) 1 « Le contrôle et le risque des systèmes d'information » / IIA, IFACI, 2ème édition, mars 2013
  - Global Technology Audit Guide (GTAG®) 4 « Management de l'audit des systèmes d'information » / IIA, IFACI, 2ème édition, mars 2013
  - Global Technology Audit Guide (GTAG®) 17 « Auditing IT Governance » / IIA, juillet 2012
  - Guide pratique : « Elaborer le plan stratégique de l'audit interne » / IIA, IFACI, juillet 2012
  - Global Technology Audit Guide (GTAG®) 7 « L'infogérance » / IIA, IFACI, 2ème édition, juin 2012
  - Global Technology Audit Guide (GTAG®) 15 « Information Security Governance » / IIA, juin 2010
  - Prise de position de l'IIA sur les ressources de l'audit interne, janvier 2009
  - Global Technology Audit Guide (GTAG®) 13 « Fraud Prevention and Detection in an Automated World » / IIA, décembre 2009
  - Guide Pratique : « L'audit des relations avec les partenaires externes » / IIA, IFACI, septembre 2009
  - Global Technology Audit Guide (GTAG®) 12 « Audit des projets des SI » / IIA, IFACI, mars 2009
  - Global Technology Audit Guide (GTAG®) 10 « Gestion de la continuité d'activité » / IIA, IFACI, juillet 2008
  - Global Technology Audit Guide (GTAG®) 11 « Elaborer le plan d'audit des SI » / IIA, IFACI, juillet 2008
  - Global Technology Audit Guide (GTAG®) 9 « Gestion des identités et des accès » / IIA, IFACI, novembre 2007
  - Global Technology Audit Guide (GTAG®) 8 « Audit des contrôles applicatifs » / IIA, IFACI, juillet 2007
- Cahier de la recherche - L'audit des Délégations de Service Public / Groupe Professionnel « Collectivités territoriales », 2015

© IFACI

- COSO : Référentiel de contrôle interne - Principes de mise en œuvre et de pilotage / Pwc, IFACI - Eyrolles, 2014
- A global look at IT audit best practices / ISACA, PROTIVITI, 2014
- eSourcing Capability Model pour les organisations clientes (eSCM-CL) / Bill Hefley, Ethel Loesche. Translated by Eric Baussand and Eric Herr, mai 2014
- White paper : Managing the outsourced internal audit function / IIA South Africa, 2013
- Cloud computing et protection des données /AFAI, IFACI, CIGREF, mars 2013
- Navigating the path from information security practionner to porfessionnel / ISACA Journal volume 4 , 2013
- Global Technology Audit Guide (GTAG®) 17 « Auditing IT Governance » / IIA, juillet 2012
- COBIT 5.0 « Un référentiel orienté affaires pour la gouvernance et la gestion des TI de l'entreprise » / ISACA, 2012
- Gouvernance du système d'information / CIGREF, IFACI, octobre 2011
- The outsourcing relationship / Internal Auditor, juin 2011
- Monitoring Internal Control Systems and IT / ISACA, 2010
- Outsourced IT Environments Audit / Assurance Program / ISACA, 2009
- Le contrôle interne du système d'information des organisations / IFACI, CIGREF, février 2009
- Generic Application Audit / Assurance Program / ISACA, 2009
- Guide d'audit des applications informatiques / ISACA, AFAI, 2008
- Audit des prestations essentielles externalisées par les établissements de crédit et les entreprises d'investissement [Cahier de la recherche] / Groupe « Banque », 2008

© IFACI

Réalisation : Ebzone Communication (www.ebzone.fr)