GTAG®

GUIDE PRATIQUE D'AUDIT DES TECHNOLOGIES DE L'INFORMATION

Élaboration d'un plan d'audit des SI

The Institute of Internal Auditors

Cette série de guides, rédigés dans des termes simples et traitant chacun d'un thème d'actualité concernant la gestion, le contrôle et la sécurité des SI, constitue un précieux outil pour les responsables de l'audit interne, qui peuvent ainsi s'informer sur les différents risques associés aux technologies de l'information et sur les pratiques recommandées.

Les contrôles des systèmes de l'information
Les sujets abordés passent en revue les concepts du contrôle des SI, l'importance de ces contrôles, les rôles et responsabilités dans l'organisation susceptibles d'assurer l'efficacité du contrôle des SI et des techniques de supervision.

Contrôles de la gestion du changement et des patchs : un facteur clé de la réussite pour toute organisation
Décrit les sources de changements et leurs impacts probables sur les objectifs de l'entreprise, explique en quoi le contrôle du processus de gestion des changements participe à la réduction des risques et des coûts des SI, et indique ce qui, dans la pratique, fonctionne ou pas.

Audit continu : Répercussions sur l'assurance, le pilotage et l'évaluation des risques
Traite du rôle de l'audit continu dans l'environnement actuel d'audit interne, de la relation entre audit continu, surveillance continue et assurance continue, précise où s'applique l'audit continu et examine la mise en place de l'audit continu.

Management de l'audit des systèmes d'information
Définit les risques liés aux SI et l'univers d'audit, explique comment conduire un audit des SI et gérer les ressources d'audit.

Le management et l'audit des risques d'atteinte à la vie privée
Présente les principes et le cadre de protection de la vie privée, un modèle de risques d'atteinte à la vie privée et le contrôle du respect de la vie privée, le rôle de l'audit interne, les dix questions à se poser concernant la protection de la vie privée lors de la mission d'audit, et bien plus encore.

Gérer et auditer les vulnérabilités des technologies de l'information
Analyse, entre autres, le cycle de gestion des vulnérabilités, la délimitation de l'audit des vulnérabilités et des indicateurs qui permettent d'évaluer les pratiques de gestion des vulnérabilités.

L'infogérance
Examine comment choisir le bon prestataire de services d'infogérance et présente les principaux éléments à prendre en compte pour la maîtrise de l'infogérance, du point de vue des activités du client et de celles du prestataire de services.

Audit des contrôles applicatifs
Définit la notion de contrôles applicatifs et les compare aux contrôles généraux informatiques, et indique comment déterminer l'étendue des revues de contrôles applicatifs.

Gestion des identités et des accès
Couvre les principaux concepts relatifs à la gestion des identités et des accès, les risques y afférents, détaille l'audit du programme de gestion des identités et des accès et présente un exemple de liste de contrôles à l'intention des auditeurs.

Gestion de la continuité d'activité
Définit la continuité d'activité, examine les risques pour l'entreprise et propose une analyse détaillée des impératifs associés au programme de continuité d'activité

La série complète peut être téléchargée sur le site Web de l'IIA : www.theiia.org/technology.

Élaboration d'un plan d'audit des SI

Auteurs

Kirk Rehage, Chevron Corporation

Steve Hunt, Crowe Chizek and Company LLC

Fernando Nikitin, Banque interaméricaine de développement

Juillet 2008

Copyright © 2008 par l'Institute of Internal Auditors, 247 Maitland Avenue, Altamonte Springs, Florida 32701-4201, États-Unis. Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, stockée dans un système de consultation ou transmise sous quelque forme que ce soit, ni par aucun moyen (électronique, mécanique, reprographie, enregistrement ou autre), sans l'autorisation préalable de l'éditeur.

L'IIA publie ce document à titre informatif et pédagogique. Cette publication entend donner des informations, mais ne se substitue en aucun cas à un conseil juridique ou comptable. L'IIA ne fournit pas ce type de service et ne garantit, par la publication de ce document, aucun résultat juridique ou comptable. En cas de problèmes juridiques ou comptables, il convient de recourir à l'assistance de professionnels.

Sommaire

1. RÉSUMÉ 1

2. INTRODUCTION 3

2.1 Processus d'élaboration du plan d'audit des SI 4

3. PRENDRE EN COMPTE L'ACTIVITÉ 5

3.1 Une organisation unique 5

3.2 L'environnemnt opérationnel 5

3.3 Facteurs liés à l'environnement des SI 6

4. LES RISQUES DE L'ENTREPRISE 10

4.1 Examiner le modèle d'activité 10

4.2 Rôle des technologies d'appui 10

4.3 Plans d'activité annuels 10

4.4 Fonctions SI centralisées/décentralisées 11

4.5 Les processus de soutien des SI 11

4.6 Conformité à la réglementation 12

4.7 Définir les domaines soumis à l'audit 12

4.8 Les applications 13

4.9 Évaluer les risques 13

5. PROCÉDER À UNE ÉVALUATION DES RISQUES 14

5.1 Le processus d'évaluation des risques 14

5.2 Hiérarchiser les risques 15

5.3 Principaux cadres de gouvernance des SI 16

6. FORMALISER LE PLAN D'AUDIT DES SI 19

6.1 Contexte du plan d'audit 19

6.2 Demandes des parties prenantes 20

6.3 Fréquence des audits 20

6.4 Principes relatifs au plan d'audit 21

6.5 Le contenu du programme d'audit des SI 21

6.6 Intégration du programme d'audit des SI 22

6.7 Validation du programme d'audit 22

6.8 La nature dynamique du programme d'audit des SI 23

6.9 Communiquer, obtenir le soutien de la direction et faire approuver le programme d'audit 24

7. ANNEXE : EXEMPLE D'UNE ENTREPRISE FICTIVE 26

7.1 L'entreprise 26

7.2 Le plan d'audit des SI 26

GLOSSAIRE 32

LISTE DES ACRONYMES 34

À PROPOS DES AUTEURS 35

1. Résumé

À l'heure où la technologie fait plus que jamais partie des activités et opérations d'une organisation, les auditeurs internes se heurtent à une difficulté de taille : quelle est la meilleure approche pour évaluer, à l'échelle de toute l'organisation, les risques liés aux SI et les contrôles y afférents dans le cadre de leurs missions générales d'audit et de conseil ? C'est pourquoi les auditeurs doivent prendre en compte l'environnement des systèmes d'information (SI) de l'organisation, les applications et productions qui font partie de l'infrastructure des SI, le mode de gestion des applications et opérations des SI et la relation entre ces applications/opérations des SI et l'organisation.

En recensant les composants de l'infrastructure SI, l'auditeur obtiendra des informations concernant les vulnérabilités de l'infrastructure. « *L'évaluation des vulnérabilités au sein des infrastructures SI, qui sont susceptibles d'avoir une influence sur le système de contrôle interne, commence par un inventaire complet du matériel, des logiciels, des réseaux et des données. Ainsi, les systèmes et réseaux connectés à Internet sont exposés à des menaces supplémentaires par rapport à ceux qui ne le sont pas.*[1] » Dès lors que l'environnement des SI est bien pris en compte, le responsable de l'audit interne et l'équipe d'audit interne peuvent procéder à l'évaluation des risques et établir un plan d'audit.

De nombreux facteurs organisationnels entrent en ligne de compte lors de l'élaboration du plan d'audit, tels que le secteur dans lequel travaille l'organisation, son chiffre d'affaires, le type et la complexité de ses processus ou encore la localisation géographique de ses opérations. Deux facteurs ont une incidence directe sur l'évaluation des risques et sur la définition de ce qu'il convient d'auditer au sein de l'environnement du SI : les composantes et le rôle de ce dernier. Par exemple :

- Quelles technologies sont employées pour supporter les fonctions opérationnelles quotidiennes ?
- L'environnement du SI est-il relativement simple ou complexe ?
- L'environnement du SI est-il centralisé ou décentralisé ?
- Dans quelle mesure les applications sont-elles personnalisées ?
- Les activités de maintenance des SI en général ou bien certaines en particulier sont-elles externalisées ?
- A quel niveau se situe l'évolution annuelle du SI ?

Ces facteurs liés aux SI sont quelques-uns des aspects que les responsables de l'audit interne et les auditeurs internes doivent prendre en compte pour pouvoir évaluer correctement les risques de l'organisation afin d'établir le plan annuel d'audit.

De surcroît, il est important que le responsable de l'audit interne et les auditeurs internes recourent à une approche qui détermine précisément la probabilité de survenance des risques et leurs impacts en relation avec l'activité de l'organisation et qui définisse les domaines à risque élevé, moyen et faible, via des analyses quantitatives et qualitatives.

Il y a en permanence des innovations et des évolutions dans le domaine des SI. Malheureusement, ces changements peuvent entraver les efforts des auditeurs visant à identifier et à évaluer l'impact des risques. Pour aider les auditeurs informatiques, les responsables de l'audit interne peuvent :

- mesurer chaque année l'évolution spécifique de la mise en œuvre des technologies de l'information (TI), afin d'identifier celles qui pourraient avoir une incidence sur l'exposition aux risques de l'organisation ;
- prendre connaissance chaque année des plans à court terme du département informatique, et déterminer quelles peuvent en être les conséquences sur l'évaluation des risques liés aux SI ;
- commencer chaque audit des SI en actualisant l'évaluation des risques associés ;
- faire preuve de souplesse vis-à-vis de l'univers d'audit des SI ; surveiller le profil de risque de l'organisation et être prêt à adapter les procédures d'audit à son évolution[2].

Il existe plusieurs référentiels de gouvernance des SI susceptibles d'aider les responsables de l'audit interne et les équipes d'audit interne à définir l'approche d'évaluation du risque la mieux appropriée. Ces référentiels peuvent, en outre, aider les auditeurs à déterminer où se situent les risques au sein de l'environnement et donner des orientations sur la manière de gérer ces risques. Parmi les référentiels de gouvernance des SI les plus courants, citons COBIT, ITIL (IT Infrastructure Library de l'Office of Government Commerce britannique) et la série des normes 27000 de l'Organisation de normalisation internationale (ISO).

Le responsable d'audit interne et les auditeurs internes vont pouvoir déterminer les domaines à auditer et la fréquence en se basant sur une cartographie des processus, l'inventaire et la prise en compte de l'environnement du SI et l'évaluation des risques à l'échelle de l'organisation. Ce GTAG donne des informations susceptibles d'aider ces intervenants à identifier les domaines d'audit liés à l'environnement du SI comme faisant partie intégrante de son univers d'audit.

Étant donné que le fonctionnement de l'organisation dépend fortement des SI, il est essentiel en effet que le responsable de l'audit interne et les auditeurs internes

[1] GTAG 1 Les contrôles des systèmes de l'information, p. 19.
[2] GTAG 4 Management de l'audit des systèmes d'information, p. 7-8.

sachent comment élaborer un plan d'audit et pour chaque élément quelle doit en être la fréquence, ainsi que l'étendue et la profondeur.

A cette fin, le présent GTAG peut aider les responsables de l'audit interne et les auditeurs internes à :

1. prendre en compte l'activité générale de l'entreprise et la part des SI dans le support opérationnel ;
2. définir et prendre en compte l'environnement de SI ;
3. identifier le rôle de l'évaluation des risques dans la délimitation de l'univers d'audit interne ;
4. formaliser le plan annuel d'audit des SI.

Enfin, ce GTAG utilise l'exemple d'une organisation fictive pour montrer aux responsables de l'audit interne et aux auditeurs internes comment mettre en œuvre les étapes nécessaires à la délimitation de l'univers d'audit.

2. Introduction

L'une des principales attributions du responsable de l'audit interne, qui est aussi l'une de ses missions les plus délicates, consiste à élaborer un plan d'audit pour l'organisation. Comme l'explique la Norme 2010 de l'IIA (The Institute of Internal Auditors), « *le responsable de l'audit interne doit établir une planification fondée sur les risques* » au moins une fois par an, afin de déterminer les priorités d'intervention, qui doivent elles-mêmes se conformer aux stratégies et objectifs de l'organisation. En outre, le responsable de l'audit interne doit envisager des missions de conseil en fonction de la valeur ajoutée qu'elles pourraient apporter et des progrès qu'elles pourraient induire dans les opérations et les activités de management des risques de l'organisation. Ces activités ont été documentées dans l'étude 2006 du *Common Body of Knowledge* (CBOK, base commune de connaissances) de l'IIA Research Foundation. Celle-ci a observé que presque tous les responsables de l'audit interne interrogés planifiaient leurs activités d'audit au moins une fois par an, et que 36,4 % actualisaient leur programme de missions plusieurs fois par an (figure 1).

Pour élaborer un plan d'audit fondé sur le risque, le responsable de l'audit interne devra d'abord procéder à une évaluation des risques portant sur l'ensemble de l'organisation. L'évaluation adéquate des risques liés aux SI, composante essentielle de l'évaluation globale des risques, constitue un volet essentiel de la gestion des risques. C'est un facteur déterminant pour mettre en place des programmes de missions efficients. « *Pour de nombreuses organisations, l'information et la technologie sur laquelle elle repose représentent leur actif le plus précieux. En outre, étant donné que les entreprises évoluent dans un environnement concurrentiel et en constante mutation, la direction exprime, vis-à-vis des fonctions gérant et mettant en œuvre le SI, un niveau d'exigence croissant à travers : une qualité de service en constante amélioration, des fonctionnalités et une facilité d'utilisation accrues, un raccourcissement des délais, le tout alors que les coûts doivent être comprimés.*[3] »

Quelles que soient la méthodologie retenue et la fréquence des activités de planification de l'audit, le responsable de l'audit interne et l'équipe d'audit interne devront prendre en compte l'environnement du SI avant de procéder à l'audit. La plupart des activités d'une organisation font appel à la technologie. Qu'il s'agisse de la collecte, du traitement et de la communication d'informations comptables, ou bien de la fabrication, de la vente ou de la diffusion de produits, quasiment toutes les activités d'une organisation reposent, à plus ou moins grande échelle, sur la mise en œuvre de moyens technologiques. Ces derniers ont vu leur rôle évoluer : elle n'est plus seulement un support opérationnel pour les processus de l'organisation, mais fait partie intégrante du contrôle des processus. Le contrôle interne des processus et des activités reposent ainsi de plus en plus sur la technologie, dont les déficiences ou le manque d'intégrité ont un impact important sur l'atteinte des objectifs et la réalisation des opérations de l'entreprise.

Toutefois, l'élaboration d'un plan d'audit des SI efficace, fondé sur le risque, est une tâche difficile pour les auditeurs internes, surtout lorsqu'ils n'ont pas une connaissance suffisante des SI.

Les résultats de plusieurs revues d'assurance qualité externes de l'IIA font apparaître que l'un des points faibles des activités d'audit interne concerne la réalisation d'un plan d'audit des SI. Bien souvent, au lieu de réaliser des audits fondés sur les risques, les auditeurs internes examinent ce qu'ils savent déjà ou sous-traitent à d'autres entreprises, les laissant décider de ce qu'il convient d'auditer.

Le présent guide propose des techniques pour résoudre ce problème, à savoir comment déterminer sur quoi devrait porter l'audit des SI et comment organiser ces domaines en

[3] IT Governance Institute, *Control Objectives for Information and Related Technology* (COBIT), troisième édition, p. 5.

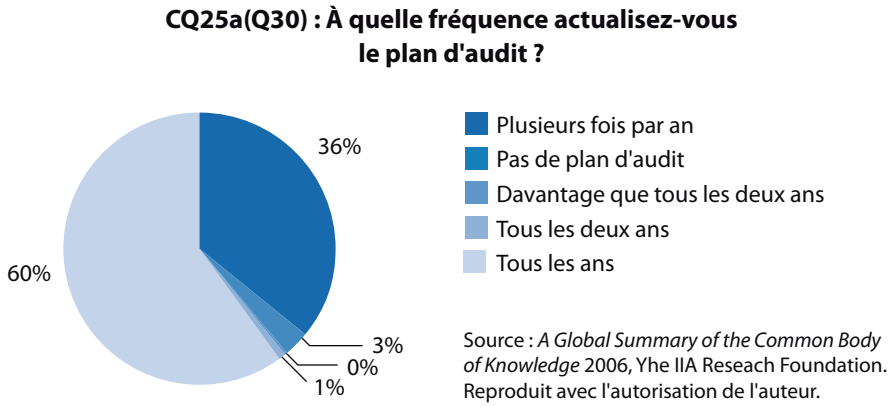

Figure 1. Fréquence des actualisations des plans d'audit.

éléments d'audit gérables, afin d'élaborer un programme de missions efficace.

2.1 Processus d'élaboration du plan d'audit des SI

La définition du plan annuel d'audit doit respecter un processus systématique si l'on veut être sûr que tous les aspects fondamentaux de l'activité et les activités de support de la DSI sont bien compris et pris en compte. En conséquence, il est essentiel que le plan s'appuie sur les objectifs, les stratégies et le modèle d'activité de l'organisation. La figure 2 décrit la progression logique des flux de travail permettant, au moyen d'une approche du général au particulier (*top-down*), de définir le plan d'audit des SI qui sera utilisé dans ce guide.

La première étape pour définir le programme de missions annuel portant sur le SI, consiste à prendre en compte l'activité de l'organisation. Durant cette étape, les auditeurs doivent identifier les stratégies, les objectifs de l'organisation et ses modèles d'activité, afin de prendre en compte les risques spécifiques associés à l'activité de l'organisation. L'équipe d'audit se doit aussi d'appréhender comment le traitement des opérations et les fonctions support de la DSI concourent à l'activité de l'organisation.

Ensuite, les auditeurs doivent définir le champ d'action spécifique de l'audit (ou univers d'audit). Ceci peut être réalisé, au moyen, d'une approche descendante qui identifie : les principaux objectifs et processus, les applications importantes qui concourent à l'activité des processus métiers, l'infrastructure supportant les traitements applicatifs, le modèle d'intervention et d'organisation de la DSI et le rôle des moyens technologiques partagés, tels que les périphériques réseau. Grâce à cette approche, associée à la prise en compte des processus de support et des projets d'implémentation, les auditeurs seront en mesure de faire un inventaire complet de l'environnement SI de l'organisation. C'est à partir de cet inventaire que se réalisera l'évaluation des vulnérabilités susceptibles d'avoir une incidence sur les contrôles internes.

Une fois que les auditeurs ont une idée précise de l'environnement du SI, la troisième étape consiste à évaluer les risques, c'est-à-dire à déterminer la probabilité de survenue d'un événement, susceptible d'empêcher l'organisation d'atteindre ses buts et objectifs de façon efficace, efficiente et maîtrisée.

Les informations et l'analyse tirées de la compréhension de l'organisation, de l'inventaire de l'environnement du SI et de l'évaluation des risques nourrissent la dernière étape, à savoir la formalisation du plan d'audit. Le plan d'audit a pour objectif de déterminer l'axe des missions d'assurance et de conseil des auditeurs afin de procurer à la direction générale des informations objectives lui permettant de gérer les risques et l'environnement de contrôle de l'organisation.

La suite de ce guide décrit ces quatre étapes et montre comment définir un plan d'audit des SI efficace.

Prendre en compte l'activité	Définir l'univers des SI	Procéder à une évaluation des risques	Formaliser le plan d'audit (programme de missions)
• Identifier les stratégies et objectifs de l'organisation • Prendre en compte ce qui présente un profil de risque élevé pour l'organisation • Prendre en compte comment l'organisation structure ses opérations • Prendre en compte le modèle de fonctionnement de la DSI comme support de l'activité de l'entreprise	• Analyser les fondamentaux de l'activité • Identifier les applications importantes qui concourent au traitement des opérations de l'organisation, en tenant compte du rôle des moyens technologiques intervenant dans ce traitement • Identifier l'infrastructure critique pour les applications importantes • Identifier les grands projets et initiatives • Définir des thèmes d'audit réalistes	• Mettre au point des processus d'identification des risques • Évaluer les risques spécifiques au SI et classer les thèmes d'audit à partir des facteurs correspondants	• Sélectionner les thèmes d'audit retenus et les grouper en missions d'audit distinctes • Définir le cycle d'audit et sa fréquence • Ajouter des missions répondant aux demandes de la direction ou constituant des opportunités pour remplir une mission de conseil • Valider le plan avec la direction

Figure 2. Le processus d'élaboration du plan d'audit des SI.

3. Prendre en compte l'activité

Il est capital de commencer avec la bonne perspective pour pouvoir définir un plan d'audit efficace. C'est pourquoi, il faut garder à l'esprit que le seul but de la technologie est de constituer un levier pour mieux atteindre les objectifs de l'organisation, sachant que toute défaillance du SI va à l'encontre de ce but et constitue un risque pour l'organisation de ne pas les atteindre. Il est donc important de commencer par prendre connaissance des objectifs, stratégies et modèles d'activité de l'organisation, ainsi que la place des moyens technologiques dans son développement. Pour ce faire, il faut identifier les risques associés aux technologies mises en œuvre, et déterminer comment chacun d'eux peut entraver la réalisation des objectifs de l'organisation. On aboutira ainsi à une évaluation plus significative et plus utile pour la direction générale.

En outre, l'auditeur doit se familiariser avec le modèle d'activité de l'organisation. Chaque organisation ayant une mission distincte et des buts et objectifs qui lui sont propres, le modèle d'activité aide l'auditeur à identifier les produits ou services que propose l'organisation, ainsi que sa base de clientèle, ses chaînes d'approvisionnement, ses processus de fabrication ou de production et ses mécanismes de mise à disposition. S'il dispose d'une connaissance approfondie de ces éléments, il pourra prendre en compte les risques spécifiques à l'organisation, ainsi que la manière dont les moyens technologiques mis en œuvre interfèrent sur le fonctionnement, comme sur l'exposition aux risques, de l'organisation.

3.1 Une organisation unique

Chaque organisation est différente. Les organisations d'un même secteur n'auront pas toutes le même modèle d'activité, des objectifs et des structures identiques, ni les mêmes environnements et schémas de mise en œuvre du SI. C'est pourquoi, les plans d'audit doivent être conçus spécifiquement pour chaque organisation. En outre, l'importance que revêt la technologie peut varier au sein d'une même branche. Prenons, par exemple, les entreprises qui assemblent et vendent des ordinateurs personnels. Outre qu'elles recourent à différents modèles d'activité, elles s'appuient de manière différente sur la technologie pour atteindre leurs objectifs. Par exemple, le modèle de distribution traditionnel consistant à passer par des magasins physiques et des revendeurs, nécessite l'utilisation d'une technologie pour gérer les opérations et la comptabilité. Les entreprises qui vendent leurs produits sur Internet sont bien plus dépendantes de la technologie. En conséquence, le flux de recettes des entreprises en ligne dépend de la disponibilité des SI critiques, ce qui augmente aussi le niveau de risques liés au SI. Comme l'illustre cet exemple, la manière dont une organisation mobilise ses ressources et moyens technologiques induit un ensemble spécifique de risques.

3.2 L'environnement opérationnel

Pour se familiariser avec une organisation, les auditeurs doivent d'abord prendre en compte les objectifs et savoir comment les processus sont structurés pour atteindre ses objectifs (figure 3).

Les auditeurs peuvent exploiter diverses ressources internes pour identifier et prendre en compte les buts et objectifs de l'organisation, notamment :

- les énoncés de la mission, de la vision et des valeurs ;
- les plans stratégiques ;
- les plans annuels de prévision de l'activité ;
- le tableau de bord de performance du management ;
- les rapports aux actionnaires et annexes ;
- les documents requis par la réglementation, tels que ceux soumis à l'autorité de contrôle prudentiel (ACP).

Une fois que les objectifs stratégiques de l'organisation au niveau de l'entité ont été bien appréhendés, l'étape suivante consiste à identifier les principaux processus critiques pour atteindre les objectifs. Pour ce faire, les auditeurs ont besoin d'appréhender en quoi chaque processus diffère au sein des directions opérationnelles, des fonctions d'appui et des grands projets à l'échelle de l'organisation, ainsi que la relation entre ces processus et les objectifs de l'entité.

Les processus liés aux projets jouent un rôle spécifique, mais tout aussi important, lorsque l'on veut s'assurer que les initiatives, créatrices de valeur pour l'organisation, sont gérées et commercialisées correctement. Un processus est qualifié de processus clé à partir du moment où son dysfonctionnement empêche l'organisation d'atteindre pleinement les objectifs auxquels ce processus est associé. Les directions fonctionnelles exécutent des processus clés par lesquels l'organisation réalise ses objectifs premiers, comme les activités de fabrication, de vente et de distribution. Les fonctions de support incluent les processus de management qui permettent de superviser et de soutenir les fonctions opérationnelles clés, comme les activités de gouvernance et de conformité, le financement, les ressources humaines, la comptabilité, la gestion de trésorerie et l'approvisionnement.

Une fois ces processus identifiés, les auditeurs dégagent les applications importantes et les infrastructures SI critiques (par exemple, les bases de données, les systèmes d'exploitation, les réseaux et les environnements physiques) qui les soutiennent. Ces applications et infrastructures, notamment le développement des systèmes, la gestion des changements, les activités opérationnelles et les activités de sécurité, sont sous-tendues par des processus d'appui des SI. Les auditeurs

devront noter que les applications appellent des évaluations périodiques, en fonction de leur importance pour la communication d'informations financières, la conformité à la réglementation ou les besoins opérationnels.

Un tel examen de l'environnement opérationnel (c'est-à-dire en partant du sommet de l'organisation) aidera les auditeurs à en appréhender et en inventorier toutes les composantes critiques. Pour pleinement prendre en compte l'environnement opérationnel et les risques associés, il faut aussi considérer chacun des facteurs technologiques qui exercent une influence sur l'exposition aux risques de l'organisation, ce qui permet de hiérarchiser ces risques.

3.3 Facteurs liés à l'environnement des SI

Pour bien prendre en compte l'environnement opérationnel et les risques qui y sont associés, différents facteurs et techniques d'analyse seront pris en considération. En effet, la complexité de l'environnement de contrôle d'une organisation aura une incidence directe sur son profil de risque global et son système de contrôle interne. Il y a plusieurs facteurs importants à prendre en compte :

1. **Le niveau de centralisation du système et de centralisation géographique (distribution des ressources SI).** Le type d'activités exercées par l'or-

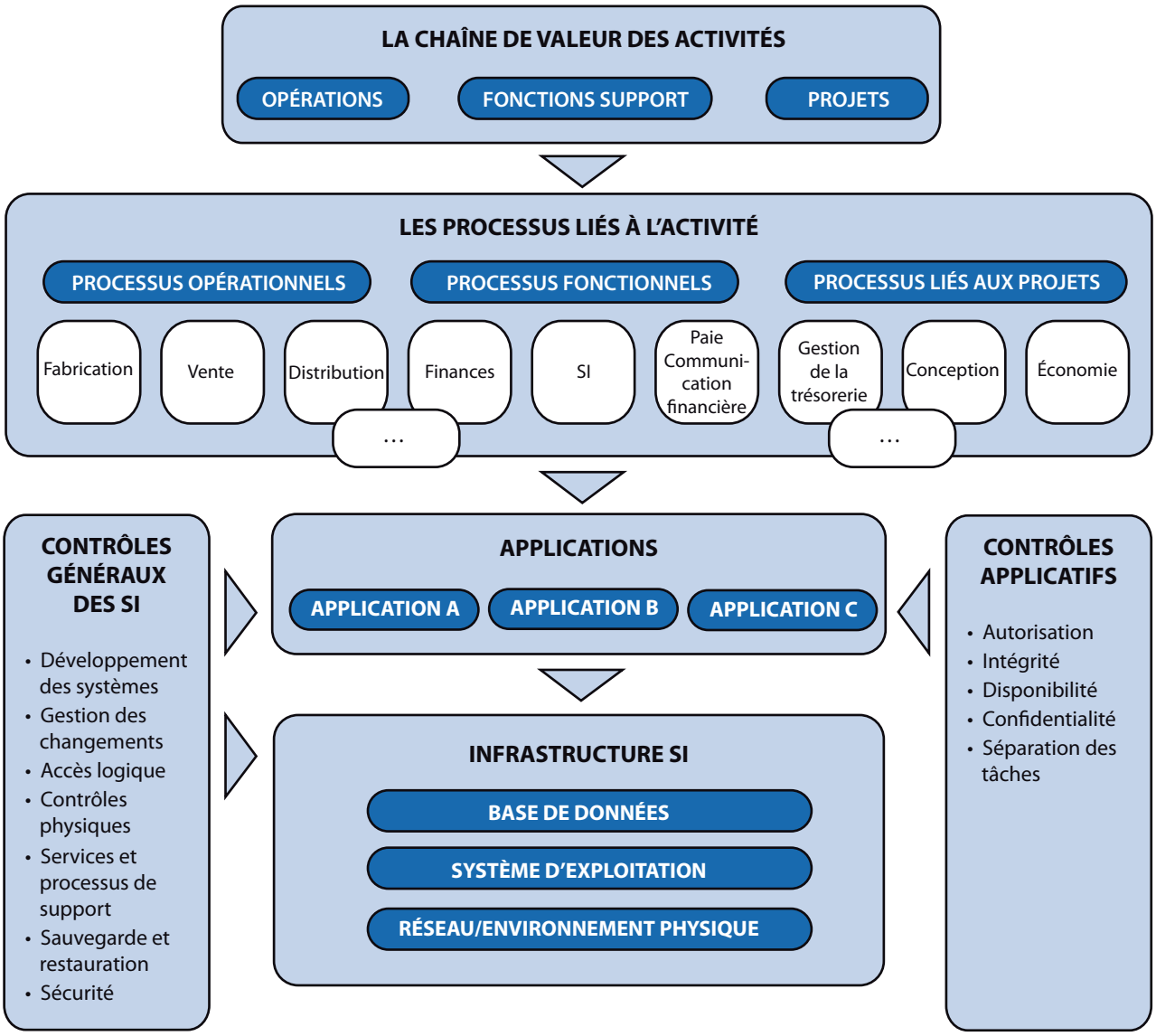

Figure tirée et adaptée de : *IT Control Objectives for Sarbanes-Oxley*, 2e édition, avec l'aimable autorisation de l'IT Governance Institute (ITGI). © 2006 ITGI. Tous droits réservés.

Figure 3. Prendre en compte l'environnement du SI de l'organisation.

ganisation peut avoir une influence sur la structure et le fonctionnement de la DSI. Par exemple, des organisations qui opèrent avec des unités d'affaires décentralisées disposant d'une certaine autonomie pour les décisions opérationnelles peuvent se caractériser par un SI décentralisé, par une plus grande diversité d'applications et par une plus grande variété de produits déployés. À l'inverse, dans les organisations plus centralisées, les auditeurs peuvent trouver des applications propres à l'organisation et une infrastructure SI centralisée. Les risques n'étant pas les mêmes selon que l'organisation se trouve à un bout ou à l'autre du spectre des possibilités de centralisation, les réponses de l'audit auront à être adaptées en conséquence.

Lorsque l'on définit l'univers d'audit des SI, il faut veiller à aligner les différents audits sur la fonction de direction qui est *in fine* responsable de ce domaine. Une organisation centralisée des systèmes d'information de l'organisation peut permettre de définir des audits moins nombreux, mais peut-être plus étendus, axés sur les technologies et les applications clés de l'organisation. À l'inverse, une organisation décentralisée *pourrait* conduire à démultiplier les missions d'audit, de façon à s'aligner sur le partage des responsabilités au niveau de la direction.

2. **Les technologies déployées.** La diversité des architectures techniques mises en œuvre dans l'organisation déterminera l'ampleur des connaissances techniques requises au sein du service d'audit interne, ainsi que le nombre de domaines spécifiques qu'il faudra examiner. Cette diversité peut se retrouver à chaque niveau de la structuration du SI « *pile de SI* », c'est-à-dire pour chaque composante principale de l'infrastructure technique d'une application : codes de programmes, bases de données, systèmes d'exploitation et infrastructure réseau.

   Ainsi, *le code d'un programme applicatif* comprend l'ensemble des programmes informatiques, fichiers de contrôle, tables et interfaces utilisateur qui lui confèrent des fonctionnalités répondant à des tâches spécifiques, telles que la comptabilité, la paie ou les achats. D'autres applications pourraient gérer des informations critiques pour l'organisation, par exemple des données sur des projets d'ingénierie, des informations juridiques ou des données médicales sur les membres du personnel. L'organisation peut également disposer d'applications qui supervisent les processus industriels, généralement appelées systèmes de « contrôle des processus ».

   Pour leur part, *les systèmes de bases de données* (SGBD) permettent le stockage, la modification et l'extraction de données (par exemple, Oracle, Microsoft SQL Server ou DB2), tandis que les systèmes d'exploitation exécutent les tâches élémentaires du traitement informatisé, notamment l'acquisition des données saisies par l'opérateur, la gestion de la mémoire interne ou celle des supports (lecture, écriture), l'affichage ou, de façon générale, tous les périphériques. Plusieurs variantes de Windows et d'UNIX peuvent être installées comme systèmes d'exploitation sur les ordinateurs et les serveurs. Les terminaux de poche, comme les assistants personnels numériques ou les téléphones cellulaires, ont également besoin d'un système d'exploitation.

   Enfin, les *réseaux* mettent en relation des serveurs et des postes de travail pour leur permettre de communiquer entre eux. Ils sont constitués de composants physiques, tels que des commutateurs, des routeurs, des pare-feux ou du câblage, et de programmes qui commandent le routage des paquets de données. Les réseaux peuvent également être déployés au moyen d'une technologie de radiofréquences. On parle alors généralement de réseaux sans fil.

   Chaque couche de structuration du SI participe au traitement automatisé de l'information, mais induit en même temps des risques relevant de la disponibilité, l'intégrité et la confidentialité des données. Le niveau de risque est fonction, d'une part, du degré d'importance pour l'organisation du domaine d'activité concerné par les moyens technologiques en cause et, d'autre part, de leur configuration comme de leur déploiement. En conséquence, plus la diversité de ces couches est grande, plus le profil de risque de l'organisation est élevé. Par exemple, le service informatique aura moins de difficultés à gérer un environnement homogène de serveurs Windows 2003, administrant une base de données avec SQL Server pour une unique application ERP (progiciel de gestion intégrée) qu'à gérer plusieurs systèmes d'exploitation et plateformes de bases de données supportant diverses applications. Même s'il paraît idéal, le premier scenario n'est guère réaliste dans une grande organisation où les opérations sont diverses et le modèle d'activité décentralisée. Lorsque l'on définit l'univers d'audit, il convient d'identifier et d'évaluer les éléments critiques des SI suivant les techniques d'analyse descendantes décrites dans le présent guide.

3. **Le degré de personnalisation.** En général, une mise en œuvre de moyens technologiques personnalisés en complexifie la gestion, tandis que l'adoption d'un logiciel standard permet de recourir essentiellement au support technique du fournisseur, qui est censé détenir une connaissance et une expertise très pointues sur ses produits. Lorsqu'un fournisseur modifie quelque chose (applications, systèmes d'exploitation ou autres logiciels), de façon à répondre aux besoins et processus de l'organisation, il en est largement propriétaire et davantage de risques sont à prendre en compte. En règle générale, les organisations doivent effectuer une analyse coûts-avantages lorsqu'elles décident d'adapter à leurs propres spécifications le logiciel d'un tiers, sans intégrer pour autant, durant cette analyse, certains aspects du contrôle. En outre, pour auditer les implémentations personnalisées, les auditeurs doivent posséder une plus grande connaissance technique.

4. **Le degré de formalisation des politiques et référentiels de l'organisation (gouvernance des SI, par exemple).** Une démarche de gouvernance des SI a pour objectif de permettre à l'organisation de mieux gérer au quotidien ses activités et risques liés aux SI aux moyens de politiques et référentiels. Ainsi, les politiques et référentiels formalisés, mis en œuvre au titre de la gouvernance des SI, contribuent à instaurer un environnement de contrôle plus efficace, ceci se vérifiant davantage si ces politiques et référentiels sont communiqués, compris, pilotés, surveillés et actualisés par la direction générale.

   Les *politiques* énoncent des principes fondamentaux, qui correspondent aux objectifs opérationnels de la direction générale ; elles entendent avoir un effet à long terme en encadrant l'élaboration des règles applicables à des domaines spécifiques, ayant pour objet de les interpréter et de les renforcer au moyen de référentiels de contrôle et de consignes. Du point de vue des SI, les politiques fournissent les directives émanant de la direction générale sur des thèmes concernant les droits attachés à la propriété intellectuelle, la protection des données, le respect de la vie privée à travers l'acquisition, la conservation ou la diffusion d'informations à caractère personnel, afin de garantir la conformité aux lois et réglementations.

   Pour leur part, les *référentiels* décrivent un processus ou une procédure obligatoire et donnent des orientations plus précises sur la manière de se conformer aux principes fondamentaux auxquels ils se réfèrent. Les référentiels portant sur les SI sont généralement neutres du point de vue de la technologie, mais peuvent être affinés au moyen de consignes et procédures (procédures ou réglages de configuration) qui définissent comment le référentiel doit être mis en œuvre vis-à-vis de telle ou telle technologie.

   En règle générale, les organisations doivent définir un processus de mise à jour continue de toutes les politiques et de tous les référentiels les plus récents que la réglementation rend obligatoires. Par exemple, les récents changements, aux États-Unis, dans les règles fédérales de procédure civile qui régissent la production de preuves devant les tribunaux portent sur la découverte et la production d'informations stockées électroniquement. En raison de ces changements, l'exposition au risque d'une organisation dépend en partie du respect des politiques et référentiels actualisés relatifs à la conservation des enregistrements, qui visent la gestion des informations stockées électroniquement.

   Il existe différents cadres et méthodologies de gouvernance des SI, dont le COBIT, la Norme ISO 27002 sur le management de la sécurité de l'information, le référentiel « La gestion du contrôle de l'informatique » de l'Institut canadien des comptables agréés (ICCA) et la norme *Standard of Good Practice for Information Security* de l'Information Security Forum. Ces référentiels méthodologiques permettent de spécifier les objectifs et domaines de contrôle dans l'ensemble de l'environnement de contrôle[4]. Les organisations peuvent adopter l'un de ces référentiels ou s'en inspirer pour développer leur propre dispositif de gouvernance du SI. La section 5.3 propose des informations sur les bonnes pratiques en la matière, afin d'aider les organisations à évaluer le contenu et l'efficacité de ces référentiels.

5. **Le degré de réglementation et de conformité.** Dans les secteurs fortement réglementés, les organisations présentent généralement un profil de risque élevé en regard des conséquences potentielles de non-conformité par rapport aux exigences réglementaires auxquelles elles sont soumises. Toutefois, les organisations qui réussissent dans des secteurs fortement réglementés se caractérisent également par un environnement de contrôle très développé intégrant une supervision efficace de la part de la direction générale, le tout étant susceptible de conférer une conformité permanente se traduisant par une exposition au risque moins élevée. Les exigences réglementaires pesant sur l'organisation doivent donc être

[4] Pour des informations complémentaires sur ces référentiels et d'autres, voir le GTAG 5 *Contrôle des systèmes d'information*, p. 23.

prises en compte, de manière appropriée, dans le niveau d'exposition au risque de l'organisation et dans l'univers d'audit des SI. Par exemple, aux États-Unis, toutes les organisations enregistrées auprès de la SEC doivent, aux termes de la loi Sarbanes-Oxley de 2002, faire état de l'efficacité de leurs contrôles internes relatifs à la communication d'informations financières. Cette législation a également instauré le Public Company Accounting Oversight Board (PCAOB), qui a pour objet de guider les commissaires aux comptes dans la manière d'auditer ce type de contrôles internes. Parmi les autres réglementations, on peut citer l'Accord de Bâle (Bâle II), qui s'applique au secteur financier, ainsi qu'un nombre croissant de lois et réglementations sur la protection de la vie privée et des données, telles que la directive européenne sur la protection des données, la loi américaine *Gramm-Leach-Bliley* (GLBA), la loi *Health Insurance Portability and Accountability* (HIPAA) et le *Payment Card Industry Data Security Standard* (PCI DSS).

6. **Le degré et le mode d'externalisation.** Le recours à l'infogérance progresse dans beaucoup d'organisations, en raison du coût élevé et de l'expertise requise pour les services sous-traités qui ne font pas partie du cœur de métier de l'organisation (le GTAG : *L'Infogérance* propose une analyse détaillée des différents modes d'infogérance et du niveau de risque qui y est associé[5]). S'agissant de l'infogérance, il est important que les auditeurs prennent en compte les différents risques émanant du mode d'externalisation lorsqu'ils élaborent leur plan d'audit des SI. Les principaux facteurs qui interviennent sont la manière dont la direction générale envisage son rôle de supervision et de pilotage, la maturité du dispositif (par exemple, processus en phase d'installation ou bien consolidé), les risques spécifiques au pays, ainsi que la complémentarité des plans de continuité d'activité à la fois de l'organisation et du prestataire.

7. **Le degré de standardisation des opérations.** Les processus et procédures opérationnelles recouvrent l'ensemble du cycle de développement des systèmes, ainsi que les activités de gestion des configurations, des changements, des incidents, des opérations et de la sécurité. À l'instar du degré de centralisation et de diversité des technologies déployées, le niveau de standardisation des opérations peut avoir une incidence sur la fiabilité et l'intégrité de l'infrastructure SI et sur chacun de ses composants. Par conséquent, les organisations qui adoptent des processus standardisés sur l'ensemble des fonctions de prestation de services améliorent leur capacité à opérer en tant qu'organisation hautement performante.

   L'ITIL, ensemble de concepts et de techniques pour la gestion des infrastructures SI, ainsi que pour le développement et la mise en place d'un nouveau système informatique et le traitement automatisé des informations, est un exemple de pratique standardisée. Les publications de l'ITIL les plus largement utilisées et comprises sont celles se rapportant à la prestation de service et l'activité de support. L'un des principaux avantages de l'ITIL est qu'il établit un glossaire commun de termes couramment utilisés. Les organisations qui mettent en œuvre les concepts de l'ITIL affichent une fiabilité plus grande et des coûts de prestation moins élevés.

8. **Le degré de dépendance technologique.** Certaines organisations sont de grandes utilisatrices de technologies ou les utilisent pour se démarquer de leurs pairs ou de leurs concurrents. Si un recours accru aux technologies de traitement de l'information peut améliorer globalement le système de contrôle interne, en particulier grâce aux contrôles applicatifs automatisés, plus la dépendance aux SI est importante, plus une forte gouvernance et de solides processus opérationnels internes sont nécessaires. En outre, lorsque les organisations dépendent fortement de la disponibilité et de l'intégrité des fonctions automatisées à travers le SI, pour traiter leurs opérations et atteindre leurs objectifs, la part des risques liés aux SI dans le profil de risque général de l'organisation augmente. Par conséquent, la nature et le degré de dépendance de l'organisation vis-à-vis de la technologie doivent être mis en exergue dans l'évaluation des risques constituant un préalable pour l'élaboration du plan d'audit des SI.

Ces huit facteurs liés à l'environnement de SI, conjugués à l'approche descendante employée pour prendre en compte les traitements opérationnels et l'infrastructure SI, constitue un socle indispensable pour passer à l'étape suivante du processus de planification de l'audit, à savoir la définition de l'univers d'audit et l'évaluation des risques.

[5] GTAG 7 : *L'Infogérance.*

4. Définir l'univers d'audit des SI

Définir ce qu'il convient d'auditer est l'une des tâches les plus importantes de l'audit interne, étant donné que le programme annuel d'audit des SI aura un impact considérable sur la performance globale du service d'audit interne. Par conséquent, le but ultime du plan d'audit des SI est d'assurer une couverture adéquate des domaines qui représentent la plus grande exposition au risque et, ceux qui représentent un enjeu majeur pour les auditeurs dans l'apport qu'il constitue en matière de valeur ajoutée à l'organisation.

L'une des premières étapes vers un plan d'audit des SI efficace consiste à définir *l'univers d'audit des SI*, c'est-à-dire un ensemble fini et exhaustif des domaines d'audit, schéma structurel des entités opérationnelles et localisation des activités réalisées par l'organisation, qui représentent les cibles d'audit permettant de donner une assurance appropriée sur le niveau de maîtrise des risques auxquels l'organisation est exposée. Lors de cette première étape, l'identification des domaines d'audit potentiels, au sein de l'univers d'audit, se fait indépendamment du processus d'évaluation des risques. Les auditeurs auront conscience des audits qui peuvent être réalisés avant de réaliser une évaluation et une hiérarchisation des risques aboutissant à un programme annuel d'audit. La définition de l'univers d'audit des SI nécessite une connaissance approfondie des objectifs de l'organisation, du modèle d'activité et des prestations assumées par la DSI.

4.1 Examiner le modèle d'activité

Pour les organisations, l'atteinte des objectifs repose sur le fonctionnement des diverses directions opérationnelles et fonctionnelles, à travers les processus spécifiques qu'elles ont à gérer afin d'atteindre leurs propres objectifs, en liaison néanmoins avec les autres entités. Si l'on revient à l'exemple des entreprises qui assemblent et vendent des ordinateurs, une entreprise traditionnelle dans ce secteur se compose de plusieurs usines d'assemblage situées dans différents pays, d'unités de vente et de marketing, ainsi que de différentes fonctions de gestion et de support. Les directions de vente et marketing, par exemple, ont mis en place des processus pour accepter, réaliser et facturer les commandes clients, alors que d'autres directions opérationnelles et fonctions support ont leurs propres processus. Les infrastructures de support et les applications critiques des SI sous-tendent ces processus. En conséquence, il est important que les auditeurs tiennent compte de l'environnement de SI de l'entreprise lorsqu'ils définissent l'univers de SI et identifient les processus fondamentaux caractérisant l'activité de chaque entité.

Le recours à une approche descendante pour prendre en compte la structure et les activités d'une organisation peut aider les auditeurs à identifier les processus de fonctionnalité critiques des SI. Néanmoins, les écarts dans la manière dont des directions similaires exécutent leurs processus peuvent ajouter à la complexité de cette analyse. Ainsi, des usines situées dans des endroits différents peuvent ne pas recourir aux mêmes procédures d'approvisionnement. Dans des organisations décentralisées, les diverses directions peuvent employer des applications différentes ou bien une application commune peut être configurée différemment dans la mesure où elle fonctionne comme une application totalement distincte. Par exemple, une unité utilise SAP R/3 sous UNIX avec une plateforme Oracle, alors qu'une autre utilise SAP R/3 sous Windows avec une plateforme SQL Server. Bien que similaire, la structure du traitement automatisé, pour ces processus, est différente et peut nécessiter des revues particulières.

4.2 Rôle des technologies d'appui

Il peut être simple d'identifier les infrastructures technologiques qui soutiennent le SI lorsque l'on détecte des activités qui reposent sur des applications clés. En revanche, il est bien plus difficile de mettre l'utilisation des moyens technologiques communs, comme le réseau général, une application de messagerie électronique ou son logiciel de chiffrement, en relation avec les objectifs et les risques. Pourtant, ces moyens technologiques communs existent parce que l'organisation en a besoin et une défaillance de ces services et équipements peut empêcher l'organisation d'accomplir sa mission. C'est pourquoi, les moyens technologiques communs clés doivent être identifiés et représentés dans l'univers des domaines auditables, même s'ils ne sont pas directement associés à une application ou à un processus opérationnel.

4.3 Plans d'activité annuels

Un autre point est important : il faut tenir compte du plan stratégique de l'organisation. Les plans opérationnels peuvent apporter aux auditeurs des informations sur les changements et projets importants susceptibles de voir le jour dans l'année à venir, qui pourraient nécessiter l'intervention de l'audit et devenir des sujets à intégrer dans l'univers d'audit des SI. Les projets peuvent avoir directement trait aux SI, par exemple la mise en œuvre d'un nouveau système d'ERP, ou porter sur la gestion d'initiatives majeures d'ingénierie ou de construction. Par exemple, les compagnies productrices d'énergie forment des projets majeurs d'investissement lorsqu'elles déploient de nouvelles installations pour exploiter de nouveaux gisements de gaz ou de pétrole. Ces projets peuvent tirer parti de l'utilisation de composantes du SI qui méritent l'attention de l'auditeur des SI, notamment les contrôles d'accès à des systèmes de gestion

de documents ou des connexions externes pour les partenaires et sous-traitants. Parce que des entreprises peuvent être partenaires sur un projet et concurrentes sur d'autres, il est important de limiter leur accès aux seules ressources SI nécessaires en l'occurrence.

4.4 Fonctions SI centralisées / décentralisées

Les auditeurs auront à identifier les fonctions SI administrées au niveau central, qui soutiennent la totalité ou une grande partie de l'organisation. Les fonctions centralisées sont de bons « candidats » aux différents audits réalisés au sein de l'univers d'audit des SI. Il s'agit notamment de la conception et de l'administration de la sécurité du réseau, de l'administration des serveurs, de la gestion des bases de données, des activités de service ou d'assistance et des opérations traitées sur des sites centraux (*mainframe*). Par exemple, l'organisation peut disposer d'un groupe d'administration serveur qui supervise l'ensemble des serveurs Windows. Parce que ce groupe peut mettre en œuvre des processus administratifs et gérer des configurations portant sur l'ensemble des serveurs, c'est le candidat idéal à un audit spécifique, qui s'intègre néanmoins dans l'univers d'audit des SI. L'homogénéité de l'environnement se prête également à un échantillonnage aux fins de la réalisation de l'audit.

L'identification des thèmes d'audit centralisés présente plusieurs avantages. Le principal est l'utilisation efficace des ressources d'audit des SI, qui sont limitées, de sorte que l'équipe d'audit peut se concentrer sur un domaine, employer des techniques d'échantillonnage et obtenir une couverture assez importante à partir d'un unique audit. Un autre atout réside dans l'intégration des résultats dans d'autres missions d'audit, afin de faire l'économie de nouvelles investigations puisque les domaines centralisés ont déjà été vérifiés ; ces avantages se vérifient tout particulièrement dans le cas des audits d'applications. Ainsi, un environnement constitué d'un groupe d'administration des serveurs Windows peut recouvrir plusieurs centaines d'applications. Puisque les contrôles généraux de l'infrastructure sont examinés au cours d'un audit (davantage) centralisé, l'audit des SI peut se limiter aux domaines techniques spécifiques à certaines applications, et non à toutes les plates-formes qui supportent l'application. L'organisation en tire également parti, dans la mesure où cet audit n'est réalisé en profondeur qu'une seule fois et que ses résultats ne risquent pas d'être impactés par l'examen individuel de chaque application, dans le cadre de l'audit d'un processus déterminé.

En outre, les organisations ne centralisent pas toutes leurs fonctions SI de la même manière. Beaucoup d'organisations choisissent de créer une unique fonction transversale réseau, en charge de la conception et de l'administration de la sécurité du réseau. Cette fonction peut se décliner en diverses activités comme la configuration des pare-feux, routeurs et commutateurs, la gestion de la connexion Internet, des réseaux sans-fil, de la voix numérique et des connexions aux réseaux externes. En conséquence, chacun de ces domaines peut constituer un domaine d'audit spécifique au sein du SI. De surcroît, parce que les fonctions SI centralisées sont susceptibles de changer au fil du temps, il convient de les examiner et de les réexaminer au moins une fois par an, parmi les thèmes relevant de l'univers d'audit du SI.

On peut adopter une approche comparable pour les fonctions SI décentralisées, pour lesquelles chaque site physique peut représenter un sujet d'audit distinct. Selon la taille du site visé, l'audit peut porter sur les contrôles généraux et les contrôles techniques, pour chaque couche de l'infrastructure. L'audit ne doit porter, toutefois, que sur les contrôles des SI dont le site local est responsable, et pas sur les contrôles gérés par les fonctions SI centralisées. Si le site est important et qu'il utilise un grand nombre de technologies, les auditeurs peuvent être amenés à réaliser plusieurs interventions dans ce site en tant que partie de l'univers d'audit.

4.5 Les processus de soutien des SI

Même si l'organisation comporte une fonction SI décentralisée, elle peut disposer de processus transversaux standardisés. Les organisations qui s'efforcent d'être performantes comprennent l'importance de disposer de processus transversaux standardisés à travers toutes leurs directions opérationnelles, quel que soit leur type d'activité. On peut citer, comme exemples de processus transversaux standardisés, les activités du centre de service (*hotline*), les procédures de gestion des changements, des configurations, des mises en production, des incidents et autres problèmes. Le centre de service est généralement le premier point de contact auprès duquel les clients peuvent formuler une requête ou une demande de résolution de problème lié aux SI. Ce qui déclenche un processus de gestion du cycle de vie de la requête à travers une succession d'événements se rapportant à la gestion des incidents, des problèmes, des changements et des mises à jour.

Là encore, l'ITIL est l'une des principales sources définissant les meilleures pratiques pour les DSI. De nombreuses organisations appliquent les pratiques recommandées par l'ITIL ou autres processus standardisés, afin d'améliorer leur efficience et leurs performances dans la gestion de leurs fonctions liées aux SI. Les services d'audit interne doivent participer aux efforts déployés pour mettre en œuvre des processus d'appui standardisés, lorsque cela se révèle approprié, et les adapter en conséquence afin d'être en mesure d'en évaluer l'efficacité. Une démarche pourrait consister à

inscrire au programme d'audit le déploiement et la gouvernance des processus standardisés à l'échelle de l'organisation. Ces revues au plus haut niveau permettraient ainsi d'évaluer l'efficacité des processus eux-mêmes, l'efficacité des processus tels qu'ils sont déployés et l'efficacité du modèle de gouvernance de façon à s'assurer que les processus transversaux sont mis en œuvre conformément à ce qui était prévu. Une fois les processus standardisés audités, les audits de sites doivent porter davantage sur le respect local des processus eux-mêmes, plutôt que sur la mesure de leur efficacité.

4.6 Conformité à la réglementation

Diverses lois et réglementations à travers la planète, en particulier la loi Sarbanes-Oxley et Bâle II, imposent d'appliquer des contrôles internes et des pratiques de gestion du risque, ainsi que de respecter la confidentialité des données personnelles .Comme indiqué plus haut, certaines de ces réglementations imposent de protéger les informations relatives aux clients en matière de cartes de crédit (par exemple, la GLBA et la PCI DSS) ainsi que les informations médicales personnelles (par exemple l'HIPAA). Même si la plupart de ces règles ne concernent pas directement les contrôles des SI, elles supposent l'existence d'un environnement de SI soumis à un contrôle adéquat. En conséquence, ces points de la réglementation sont susceptibles d'être intégrés dans l'univers d'audit : les auditeurs doivent déterminer si l'organisation a mis en place des processus rigoureux et si elle opère efficacement afin de garantir la conformité.

4.7 Définir les domaines soumis à l'audit

La division de l'environnement des SI en plusieurs thèmes d'audit peut être quelque peu influencée par des préférences personnelles ou des considérations relatives aux effectifs. Toutefois, le but ultime est de déterminer comment scinder l'environnement de façon à obtenir les audits les plus efficients et les plus efficaces. La discussion précédente sur la centralisation des fonctions SI et la standardisation des processus de soutien montrait comment les domaines d'audit pouvaient être regroupés au sein de l'univers d'audit afin de définir une approche plus efficiente. Bien que les auditeurs n'aient pas à évaluer les risques à cette étape du processus de planification de l'audit, l'objectif est de disposer d'un plan d'audit centré sur les domaines présentant le risque le plus élevé, dans lesquels les auditeurs peuvent apporter le plus de valeur ajoutée.

Même s'il n'existe pas une façon unique de définir les objets d'audit des SI, il existe des façons incorrectes ou inappropriées de le faire[6].

Les écueils à éviter sont notamment de ne pas définir correctement le périmètre de la mission, ou de définir le plan uniquement en fonction des capacités des effectifs, ou de créer un déséquilibre dans les sujets traités.

En outre, les objets d'audit doivent être scindés en domaines de dimension appropriée à une affectation raisonnable des ressources d'audit. Ce faisant, les auditeurs garderont à l'esprit qu'une définition large ou restreinte des objets d'audit, risque d'avoir un impact positif ou négatif sur les travaux d'audit. En effet, chaque mission comporte un certain nombre de charges, notamment pour la gestion administrative ayant trait à la planification de l'audit, les revues de management, la validation finale des travaux et la formalisation et la communication des résultats. Si, par exemple, le programme d'audit prévoit de nombreuses missions à caractère restreint, les auditeurs internes pourraient passer autant de temps à gérer les audits qu'à les effectuer. À l'inverse, si le domaine audité est très large, les audits pourraient se dérouler sur une période prolongée, gêner le client ou induire un examen trop superficiel. Selon la culture de l'organisation, des définitions trop vastes pourraient même aboutir à une augmentation non planifiée du champ de l'audit (glissement de périmètre[7]).

La dimension adéquate de l'audit dépend de la culture et des pratiques de l'organisation. En règle générale, pour la plupart des organisations, définir un objet d'audit qui mobilise deux à trois auditeurs techniques semble être un objectif raisonnable, car on bénéficie alors des points de vue et expériences variés des auditeurs. En outre, une durée de trois à quatre semaines semble raisonnable pour la plupart des organisations.

La taille de l'audit doit aussi cadrer avec les pratiques d'audit en vigueur dans l'organisation. Cependant, l'univers d'audit des SI ne doit pas se définir uniquement en fonction de la structure du service d'audit en termes d'effectifs, puisque cela risquerait d'aboutir à un déséquilibre entre les missions réalisées. Ainsi, certains services d'audit informatique ne disposent d'aucun technicien ou spécialiste des SI, mais se composent d'auditeurs connaissant les applications existantes. Ces auditeurs ont tendance à se concentrer sur la couche applicative et risquent de ne pas prêter une attention suffisante aux couches d'infrastructure sous-jacentes, alors même qu'il serait nécessaire d'aboutir à une couverture bien équilibrée de toutes les couches techniques dans le cadre des missions réalisées.

Idéalement, la fonction d'audit interne doit regrouper des membres du personnel disposant d'une qualification technique pointue et des auditeurs généralistes avec une bonne compréhension des contrôles applicatifs. Les auditeurs techniques, par exemple, peuvent vérifier que l'infrastructure SI bénéficie de contrôles de sécurité adéquats et examiner les contrôles applicatifs généraux. Un bon équilibre entre les objets d'audit, qui appréhendent toutes les

[6] GTAG 4 : *Management de l'audit des systèmes d'information*, p. 11.
[7] GTAG 4 : *Management de l'audit des systèmes d'information*, p. 11.

couches de l'environnement informatique, constitue la clef de voûte du plan d'audit des SI, même si les contraintes, liées au personnel du service d'audit, sont un réel problème. Si tel est le cas, des effectifs supplémentaires sont nécessaires pour compléter l'expertise du personnel en place.

Les auditeurs doivent être conscients que la technique d'audit utilisée durant les examens de la sécurité pourrait se révéler inefficace si elle est utilisée dans un environnement de serveurs non homogène, formé de multiples plateformes. De fait, le domaine général de l'administration des serveurs pourrait être trop vaste ou ingérable.

Pour cette raison, de nombreuses organisations examinent leur sécurité en fonction du type de plateforme qui les concerne, ce qui permet une analyse plus détaillée. Malheureusement, cette activité pourrait se traduire par des doublons car certaines étapes d'audit sont répétées. En conséquence, les auditeurs doivent définir des champs d'intervention distincts pour chaque plateforme et procéder à un audit des contrôles généraux sur toutes les plateformes.

La responsabilité managériale est un point clé à prendre en considération lorsque l'on définit les composantes de l'environnement du SI. Dans le pire des scenarii, on pourrait définir des thèmes d'audit qui s'avéreraient transversaux par rapport aux lignes hiérarchiques pilotant les différentes entités opérationnelles concernées. Cela pourrait créer en conséquence un conflit quant à savoir à qui il revient, *in fine*, de mettre en application les remarques et recommandations émises par l'audit à l'issue de la mission. Il faut donc préciser clairement qui recevra le rapport d'audit et qui est chargé de remédier aux déficiences de contrôles identifiées. Enfin, le périmètre de chaque thème d'audit doit être décrit clairement, de sorte que les responsabilités en cause au sein de l'organisation soient clairement définies.

4.8 Les applications

Le responsable de l'audit interne doit déterminer quel groupe d'audit sera chargé de planifier et de réaliser l'audit des applications. Selon le mode de fonctionnement du service d'audit, les applications peuvent être incluses dans l'univers d'audit des SI, dans celui de l'organisation ou dans les deux. Les services d'audit interne s'accordent, de plus en plus, à dire que les applications doivent être auditées en même temps que les processus qu'elles supportent. On obtient ainsi une assurance sur toute la suite des contrôles, automatisés ou manuels, portant sur les processus examinés, en minimisant les risques de lacunes ou de chevauchements susceptibles d'être rencontrés au cours des travaux d'audit, et éviter autant que possible les confusions quant à ce qui fait partie ou non du champ de la mission.

En raison de leur expertise, les auditeurs sont probablement les mieux à même de déterminer le moment opportun pour examiner les applications. Si ces dernières sont maintenues dans l'univers d'audit des SI, alors l'univers d'audit de l'organisation doit être mis en relation avec celui des SI de façon à obtenir une vision globale pendant l'audit. Même si les applications sont maintenues à l'écart de l'univers d'audit des SI, des thèmes d'audit individuels peuvent être sélectionnés au sein de l'univers d'audit des SI pour les applications à grande échelle, c'est-à-dire qui sont mises en oeuvre par des fonctions multiples pour des processus multiples. En effet, il peut être intéressant d'examiner les contrôles généraux d'une application dans le cadre d'un audit autonome, plutôt qu'en l'incluant arbitrairement dans l'un des nombreux audits généraux.

4.9 Évaluer les risques

Une fois l'univers d'audit défini, l'étape suivante de la définition du programme annuel d'audit consiste en une évaluation systématique et uniforme des risques associés à tous les sujets. La section suivante présente des notions fondamentales sur les risques et leur évaluation, qui peuvent aider les responsables de l'audit interne et les auditeurs internes à créer un programme d'audit des SI efficace.

5. Procéder à une évaluation des risques

L'IIA définit le risque comme la « *possibilité que se produise un événement qui aura un impact sur la réalisation des objectifs. Le risque se mesure en termes de conséquences et de probabilité*[8]». Il est donc absolument crucial que les organisations fassent périodiquement l'inventaire des risques auxquels elles sont exposées et qu'elles entreprennent les actions nécessaires pour maintenir ces risques à un niveau acceptable. Comme indiqué plus haut, le processus d'évaluation des risques ne doit pas être mené avant que le responsable de l'audit interne et l'équipe d'audit interne aient bien identifié l'univers d'audit des SI et la place qu'il occupe au sein de l'organisation et au soutient ses activités. Il est capital, quel que soit le modèle ou l'approche d'évaluation des risques retenu, que cette évaluation cerne les domaines de l'environnement du SI susceptibles d'entraver fortement la réalisation des objectifs de l'organisation. En d'autres termes, l'évaluation des risques doit intégrer l'infrastructure, les applications et les opérations informatisées et, de façon générale, tous les composants du SI, qui pèsent le plus sur la capacité de l'organisation à veiller à la disponibilité, à la fiabilité, à l'intégrité et à la confidentialité du système et des données.

En outre, les auditeurs doivent tenir compte de l'efficacité et de la pertinence des résultats de l'évaluation des risques, lesquels dépendent de la méthode employée et de sa bonne mise en œuvre. En somme, si les données d'entrée utilisées pour évaluer les risques (c'est-à-dire l'univers d'audit des SI et sa relation avec l'univers d'audit de l'organisation) sont déficientes ou utilisées incorrectement, il est vraisemblable que les résultats de l'évaluation en seront, à certains égards, insatisfaisants.

5.1 Le processus d'évaluation des risques

Dès lors que le responsable de l'audit interne et l'équipe d'audit interne ont une bonne connaissance de l'organisation et des technologies qui y sont mises en œuvre, ils peuvent mener une évaluation des risques. Il est crucial d'exécuter ces tâches correctement si l'on veut être sûr que les risques pertinents liés aux SI (c'est-à-dire ceux qui présentent la plus grande probabilité d'occurrence et d'impact sur l'organisation) sont identifiés et évalués avec efficacité, et qu'ont été prises, de façon appropriée, des mesures destinées à les maîtriser. Le résultat du processus d'évaluation des risques sert ensuite au responsable de l'audit interne et à l'équipe d'audit interne pour élaborer un plan d'audit des SI.

5.1.1 Identifier et prendre en compte les objectifs de l'entreprise

L'un des fondements de toute méthode d'évaluation des risques consiste à prendre en compte les objectifs de l'organisation et à déterminer en quoi les SI contribuent à la réalisation de ces objectifs ou les soutiennent. Si les objectifs de l'organisation ne sont pas déjà identifiés, les auditeurs doivent le faire avant de procéder à l'évaluation des risques propres au SI. Les objectifs de l'organisation peuvent être vastes et de nature stratégique (par exemple, devenir un chef de file du secteur) ou plus linéaires et de nature plutôt tactique (par exemple, remplacer les anciennes applications SI par un système d'ERP).

En outre, les processus de gestion des risques devra passer par cinq grandes étapes :

- Il faut identifier et hiérarchiser les risques découlant des stratégies et activités de l'organisation.
- La direction générale et le Conseil d'administration définissent le niveau de risque acceptable pour l'organisation, y compris le niveau d'acceptation des risques liés aux plans stratégiques de l'organisation.
- Il convient de concevoir et de mettre en œuvre des actions concourant à la maîtrise des risques, en les réduisant ou les ramenant en tout état de cause dans les limites fixées comme acceptables par la direction générale et le Conseil d'administration.
- Il convient de mettre en place un dispositif de surveillance continue afin de réévaluer périodiquement les risques, comme l'efficacité des contrôles visant à gérer ces risques.
- Le Conseil d'administration et la direction générale reçoivent périodiquement des rapports sur les processus de gestion des risques. Les processus de gouvernement d'entreprise en place prévoient également une communication régulière aux partenaires financiers sur l'état d'exposition aux risques, les stratégies et les contrôles mis en œuvre en conséquence.

On trouvera des orientations complémentaires dans la MPA 2010-1 : La prise en compte des risques et des menaces pour l'élaboration du plan d'audit, qui indique comment les risques pour l'organisation, son plan stratégique et les changements d'orientation décidés par la direction générale sont pris en compte dans le programme d'audit.

5.1.2 Identifier et prendre en compte la stratégie relative aux SI

Une fois que le responsable de l'audit interne et les auditeurs internes sont au courant des objectifs de l'organisation, il leur faut identifier la stratégie générale de l'organisation

[8] Définition du risque issue du glossaire, Cadre de Référence International des Pratiques Professionnelles de l'audit interne, IIA-IFACI, 2009.

vis-à-vis des SI, afin de vérifier si elle cadre avec les objectifs identifiés à l'étape précédente. L'organisation peut disposer de divers documents décrivant la relation entre ses objectifs et le plan stratégique des SI, auxquels le responsable de l'audit interne et les auditeurs internes ont besoin d'avoir accès, pour en prendre connaissance et en tenir compte dans leurs travaux. De manière générale, le plan stratégique est adossé aux objectifs de l'organisation et précise de quelle manière il a été conçu en ce sens. En d'autres termes, le plan d'audit identifiera des actions tactiques qui seront effectuées par la DSI dans un délai précis, actions visant à soutenir la réalisation des objectifs de l'organisation.

5.1.3 L'univers du SI

Comme indiqué plus haut, les auditeurs commenceront par dresser l'inventaire des composantes de l'environnement informatique afin de déterminer quels domaines du SI verront leurs risques et contrôles examinés. S'il n'existe pas une approche unique idéale pour réaliser cet inventaire, de nombreuses organisations scindent leur univers de SI en trois grandes sous-catégories : infrastructure, production ou exploitation, et applications.

L'infrastructure inclut toutes les composantes techniques qui soutiennent la circulation et le traitement des informations de l'organisation, comme les serveurs, routeurs, ponts, *mainframe*, lignes de communication, imprimantes, serveurs de données, équipements réseau, antivirus et ordinateurs de bureau.

La production informatique vise, pour sa part, les processus et contrôles qui gèrent l'environnement informatique. On citera, par exemple, l'administration de la sécurité physique et logique, la sauvegarde et la récupération des données, les plans de continuité et de reprise d'activité, les contrats de service, les contrôles portant sur les changements de programme, ainsi que la conformité aux lois et réglementations. Enfin, les applications désignent les logiciels utilisés pour traiter, stocker et communiquer les données relatives aux transactions, aussi bien les systèmes d'ERP que les applications autonomes gérées avec Microsoft Excel ou Access.

5.2 Hiérarchiser les risques

Une fois achevé l'inventaire de l'univers du SI, l'étape suivante consiste à valoriser les risques associés à chacune des sous-catégories (infrastructure, production et applications) : il s'agit de classer ces sous-catégories sur la base de la probabilité d'occurrence des risques qui y sont associés, ainsi que de l'impact que ces derniers pourraient avoir sur l'organisation s'ils se matérialisaient. Autrement dit, les auditeurs détermineront les dysfonctionnements susceptibles d'intervenir pour chaque catégorie et en quoi l'organisation en sera affectée si les contrôles visant à gérer ou à atténuer ces dysfonctionnements ne sont pas appliqués correctement, ou s'ils ne fonctionnent pas efficacement.

De plus, les auditeurs garderont à l'esprit que tous les risques peuvent ne pas avoir la même importance ou être pondérés de la même manière dans l'univers d'audit des SI (la pondération permet de distinguer l'importance relative d'un risque par rapport aux autres). Ainsi, si un domaine a une incidence directe sur l'exactitude de la communication financière, il devrait être pondéré plus fortement qu'un autre qui n'affecte pas directement l'exactitude de la communication financière. D'après la publication *Assessing Risk* de l'IIA Research Foundation[9], on peut mesurer le risque et l'impact suivant trois approches :

1. **Estimation directe des probabilités et des pertes attendues, ou application de probabilités à la valeur des actifs afin de déterminer le niveau potentiel de pertes**. Ce processus est le plus ancien, et n'est pas considéré comme une bonne pratique. Si le secteur des assurances le pratique toujours, les auditeurs internes s'en abstiendront.
2. **Facteurs de risques ou utilisation de facteurs observables ou mesurables afin de valoriser un risque spécifique ou une classe de risques.** Ce processus est à privilégier pour des évaluations globales (macro) de risques, mais il n'est pas particulièrement efficace pour une évaluation élémentaire (micro) de risques, sauf lorsque les caractéristiques des unités objets d'audit sont homogènes sur l'ensemble de l'univers d'audit : une succursale, un site ou une usine, par exemple.
3. **Matrices pondérées ou de classification, ou utilisation de matrices « menaces vs composantes » afin d'évaluer les conséquences et les contrôles.** Cette méthode est préférable pour la plupart des évaluations de risques élémentaires.

Le présent GTAG se concentrera exclusivement sur l'approche par les matrices pondérées ou de classification pour mesurer le risque et son impact. Comme le montre le tableau

Échelle de probabilité		
É	3	Probabilité élevée que le risque survienne.
M	2	Probabilité moyenne que le risque survienne.
F	1	Faible probabilité que le risque survienne.

Tableau 1. Échelle des risques d'occurrence

[9] The IIA Research Foundation, *Assessing Risk*, 2e édition, 2004.

1, cette approche utilise une méthode très simple pour noter le risque, selon que la probabilité d'occurrence du risque est élevée (3), moyenne (2) ou faible (1).

Si la probabilité d'occurrence du risque est relativement simple à établir, il en va tout autrement quand il s'agit de déterminer l'impact si la menace se concrétise. En effet, l'impact du risque peut comporter plusieurs aspects quantitatifs et qualitatifs. En outre, les différents aspects ne sont pas tous traités de la même manière (certains risques sont plus importants que d'autres). D'après *Assessing Risk*[10], on distingue généralement trois types de facteurs de risques : les facteurs de risques subjectifs, les facteurs de risques objectifs ou historiques, et les facteurs de risques calculés.

1. **Les facteurs de risques subjectifs.** Pour mesurer le risque et son impact, il faut mobiliser à la fois de l'expertise, des compétences, de l'imagination et de la créativité. Cet accent placé sur les mesures subjectives est corroboré par la pratique : bien des unités auditables évoluent tellement entre deux audits que l'historique des audits antérieurs n'apporte pas grand-chose. En conséquence, le jugement censé mais subjectif d'un praticien chevronné est tout aussi valide que n'importe quelle autre méthode.
2. **Les facteurs de risques objectifs ou historiques.** La mesure des tendances des facteurs de risques peut se révéler utile dans les organisations stables. Dans tous les cas, des informations objectives actualisées sont utiles pour mesurer le risque.
3. **Les facteurs de risques calculés.** À partir d'informations historiques ou objectives, on peut établir la catégorie des facteurs de risques calculés, qui est un sous-ensemble de la catégorie précédente. Ces facteurs sont souvent les plus délicats à utiliser car ils découlent de facteurs de risques en amont.

En raison de ces facteurs de risques, les responsables de l'audit interne et les auditeurs internes conçoivent et appliquent un modèle d'impact des risques qui correspond à leur organisation. Ce modèle doit être analogue à celui employé pour l'évaluation des risques de l'ensemble de l'organisation. Cependant, l'échelle du modèle et la méthodologie de classement sont modifiées pour chaque risque lié aux SI. Comme le montre le tableau 2, et pour les besoins de ce GTAG, l'impact de chaque composante est classé selon une méthode très simple de classement des risques (catégories élevée, moyenne ou faible), comme pour la probabilité d'occurrence présentée au tableau 1.

Le tableau 3 page 18 montre un exemple de résultats d'une évaluation des risques : on a appliqué les échelles de probabilité et d'impact à chacune des catégories de risques

[10] The IIA Research Foundation, *Assessing Risk*, 2e édition, 2004.

Échelle d'impact (financier)		
É	3	Le potentiel d'impact sur les recettes, les actifs, la réputation ou les parties prenantes de l'organisation est élevé.
M	2	Le potentiel d'impact sur les recettes, les actifs, la réputation ou les parties prenantes de l'organisation peut être significatif pour le département d'audit, mais modéré pour l'ensemble de l'organisation.
F	1	L'impact potentiel sur l'organisation est d'ampleur et de portée limitées.

Tableau 2. Échelle modèle de l'impact des risques

(financiers, qualité du dispositif de contrôle interne, changements dans les unités d'audit, disponibilité, intégrité et confidentialité). Pour chaque catégorie, on multiplie la valeur attribuée à la probabilité d'occurrence de la menace par celle affectée à l'impact ; le score pour chaque domaine est égal à la somme de ces produits. Par exemple, pour les risques qui concernent le domaine de l'application ERP et contrôles généraux, la somme des valeurs obtenues pour le produit de la probabilité et de l'impact donne 42. La même procédure est appliquée à tous les autres domaines d'audit envisageables.

Sur la base de cette approche de la notation, le score le plus bas possible est 6 et le plus élevé 54. Le tableau 4 montre les fourchettes de notes et les fréquences des audits ou des revues qui y correspondent sur la base des ressources disponibles de l'organisation.

Niveau	Fourchette des scores composites du risque	Fréquence recommandée pour le cycle d'audit
É	35-54	Tous les 1 à 2 ans
M	20-34	Tous les 2 à 3 ans
F	6-19	Tous les 3 à 5 ans

Tableau 4. Fourchettes de scores et fréquences des audits et des revues correspondantes

5.3 Principaux cadres de gouvernance des SI

Jusqu'à présent, ce guide s'est concentré sur les différentes étapes nécessaires pour définir l'univers d'audit des SI et mener une évaluation des risques qui permette de déterminer ce qu'il convient d'auditer et à quelle fréquence. Cette analyse ne s'appuie pas sur un cadre de gouvernance des SI

en particulier, comme le COBIT, la norme ISO 27002 ou l'ITIL. Par conséquent, il incombe au responsable de l'audit interne de déterminer quelles parties de ces référentiels, ou d'autres, répondent le mieux aux besoins de l'organisation.

Il importe de garder à l'esprit qu'aucun de ces cadres de référence n'est applicable à toutes les situations. Il s'agit plutôt de cadres que les organisations peuvent utiliser pour gérer et améliorer les fonctions SI. Il sortirait du champ de ce GTAG de donner des indications sur les avantages et les inconvénients de ces référentiels, comme des autres modèles de gouvernance des SI, mais nous proposerons un survol du COBIT.

Depuis sa publication en 1996, le COBIT constitue un référentiel phare pour la gouvernance des SI. Sa mission est de « *concevoir, développer, publier et promouvoir un ensemble d'objectifs de contrôle de l'informatique généralement acceptés correspondant à l'état de l'art, valables au plan international et qui fassent autorité, à destination des gestionnaires et des auditeurs, pour leur usage quotidien*[11] ». Formant un cadre et un ensemble d'outils, le COBIT permet aux organisations de combler des lacunes en termes de contrôles impératifs, de problèmes techniques et de risques pour l'organisation, et de communiquer ce niveau de contrôle aux parties prenantes. Le COBIT favorise également la mise au point de politiques et de pratiques claires pour le contrôle des SI[12].

En outre, le COBIT propose aux responsables de l'audit interne et aux auditeurs internes un ensemble d'outils sur lesquels ils peuvent s'appuyer pour orienter le processus d'évaluation des risques liés aux SI. Il propose, comme outils, un ensemble d'objectifs de contrôle clairement énoncés, des solutions pour tester les contrôles, ainsi qu'une échelle pour classer la maturité de l'environnement de contrôle des SI. Le référentiel COBIT se compose de quatre domaines (planification et organisation, acquisition et mise en place, distribution et support, surveillance et évaluation) avec un total de 34 processus relevant des SI.

Comme pour n'importe quel cadre de contrôle s'appuyant sur des bonnes pratiques, les auditeurs doivent procéder avec prudence lorsqu'ils utilisent ce cadre. Le responsable de l'audit interne et les auditeurs internes doivent prendre en compte les concepts et orientations du cadre et les appliquer dans leur propre contexte. En d'autres termes, le COBIT a été élaboré, puis affiné au cours de la dernière décennie avec l'aide d'experts de terrain, d'universitaires et de différents secteurs d'activité à travers le monde. Il en résulte un référentiel qui semble pouvoir fonctionner parfaitement dans une grande organisation, disposant d'une fonction SI importante, mais qui peut fonctionner tout aussi bien dans les petites et moyennes organisations.

Toutefois, le responsable de l'audit interne et l'équipe d'audit interne doivent avoir bien conscience que ce n'est pas parce que la fonction d'audit ne suit pas à la lettre le cadre du COBIT que la DSI, ses processus ou ses données ne sont pas contrôlés ou gérés correctement. Ils peuvent simplement se servir du COBIT comme d'un guide utile durant l'évaluation des risques liés aux SI, et ensuite l'audit proprement dit. Dans le meilleur des cas, le responsable de l'audit interne et l'équipe d'audit interne peuvent intégrer le COBIT à l'ensemble des référentiels et directives relatifs aux contrôles et aux risques, ainsi que pour aider la DSI à mettre en œuvre tout ou partie du référentiel.

[11] *COBIT*, 3e édition, p. 1.
[12] *COBIT 4.1*, p. 8.

Domaine	Impact financier		Risques liés aux SI										Score et niveau	
			Qualité du dispositif de contrôle interne		Changements dans l'unité d'audit		Disponibilité		Intégrité		Confidentialité			
	P	I	P	I	P	I	P	I	P	I	P	I		
Contrôles de l'application ERP et contrôles généraux	3	3	2	3	3	3	2	3	2	3	2	3	42	É
Systèmes de transfert électronique de fonds	3	3	3	3	3	3	2	2	3	2	2	2	41	É
Applications RH/paie	3	3	3	2	3	3	2	2	2	3	2	3	40	É
Applications relatives aux avantages sociaux (externalisées)	2	3	2	2	3	3	3	2	2	3	3	3	40	É
Infrastructure SI	2	2	3	2	3	3	3	3	3	2	2	2	38	É
Systèmes de contrôle des processus	1	1	2	2	2	2	2	2	1	1	1	1	15	F
Administration et sécurité des bases de données	2	2	2	2	2	2	3	3	2	2	2	1	27	M
Administration et sécurité sous UNIX	2	2	2	3	2	2	3	1	1	1	3	2	24	M
Respect de la politique de confidentialité de l'entreprise	2	2	3	2	3	3	2	1	2	2	3	3	34	M
Administration et sécurité des serveurs sous Windows	2	2	1	2	2	2	2	3	1	1	3	1	26	M
Systèmes de reporting environnemental	2	2	2	2	2	2	1	1	2	2	1	2	24	M
Examen de la conformité à la loi SOX	2	2	1	1	1	2	2	1	2	2	2	2	19	F
Administration et sécurité du réseau	1	1	1	3	2	1	3	1	1	3	3	3	17	F
Pratiques de déploiement de l'ITIL	1	1	1	3	2	1	3	1	1	3	3	3	21	M
Pratiques de gouvernance des SI	1	1	2	2	1	1	3	1	1	1	1	2	12	F
Connectivité à distance	1	1	1	2	2	1	1	1	1	2	2	2	12	F
Contrôle des changements apportés aux programmes applicatifs	2	3	1	3	1	1	1	1	1	3	1	2	16	F

Score le plus bas possible			6											
Score le plus élevé possible			54											
Point intermédiaire			30											
P = Probabilité I = Impact														

Tableau 3. Exemple de modèle de notation pour la hiérarchisation des risques liés aux SI

6. Formaliser le plan d'audit des SI

La définition de l'univers d'audit des SI et la réalisation d'une évaluation des risques sont les étapes préalables qui permettent de définir ce qu'il faut inclure dans le plan d'audit des SI. Alors que tous les éléments de l'univers d'audit pourraient être examinés périodiquement, lorsque les ressources disponibles sont illimitées, tel n'est pas le cas pour la plupart des fonctions d'audit. Par conséquent, le responsable de l'audit interne doit créer un programme d'audit tenant compte des contraintes du budget opérationnel de la fonction d'audit et les ressources disponibles.

6.1 Contexte du plan d'audit

La figure 4 montre en quoi l'étape de l'évaluation des risques diffère de celle de l'identification des audits qui seront inclus dans le programme d'audit, ainsi que les difficultés que cela pose. En théorie, chacune de ces étapes doit constituer un travail distinct parce que les objectifs et le thème traité sont différents. Dans l'évaluation des risques, l'objectif est d'appréhender les risques dans un contexte relatif. La cible principale (axe central) en est donc le risque, tandis que les ressources disponibles peuvent constituer un facteur déterminant quant à la réalité du travail effectué. Lors de la définition du programme d'audit, l'objectif est d'examiner les domaines à risque élevé pour définir l'affectation des ressources disponibles. Dans ce cas, les ressources constituent la cible, mais les risques représentent au final le facteur décisif.

Dans la plupart des organisations, ces deux étapes fusionnent, dans une certaine mesure, comme le montre la surface de chevauchement des deux sphères représentant chaque processus dans la figure 4. Ainsi, certains risques ou domaines auditables peuvent être exclus de l'évaluation des risques sur la base du niveau de ressources qui peut être requis pour l'audit. Toutefois, il importe de réaliser ces étapes de façon objective, en tenant compte des facteurs et des objectifs de chaque étape.

En outre, le programme d'audit des SI devra être élaborer dans le cadre du processus de planification stratégique de l'audit interne. Ce processus est cyclique et peut être intégré dans un cycle de management classique « *plan, do, check, and act* » (planifier, réaliser, vérifier, ajuster). En conséquence, alors que la programmation est le principal dispositif qui permet de mettre en œuvre ce processus, elle détermine la manière d'atteindre les objectifs d'audit. Il convient en cela d'y inclure une liste des activités d'audit, le calendrier, les relations de dépendance et la répartition de ressources nécessaires pour atteindre les objectifs d'audit.

Certaines normes de l'IIA décrivent la nature des services d'audit interne et proposent des critères de qualité au regard desquels se mesure leur performance. Les critères de performance présentés dans les normes 2000 Gestion des services d'audit interne, sont tout à fait adaptés au processus de programmation de l'audit :

- **Norme 2010 – Planification.** Le responsable de l'audit interne doit établir une planification fondée sur les risques afin de définir des priorités cohérentes avec les objectifs de l'organisation.

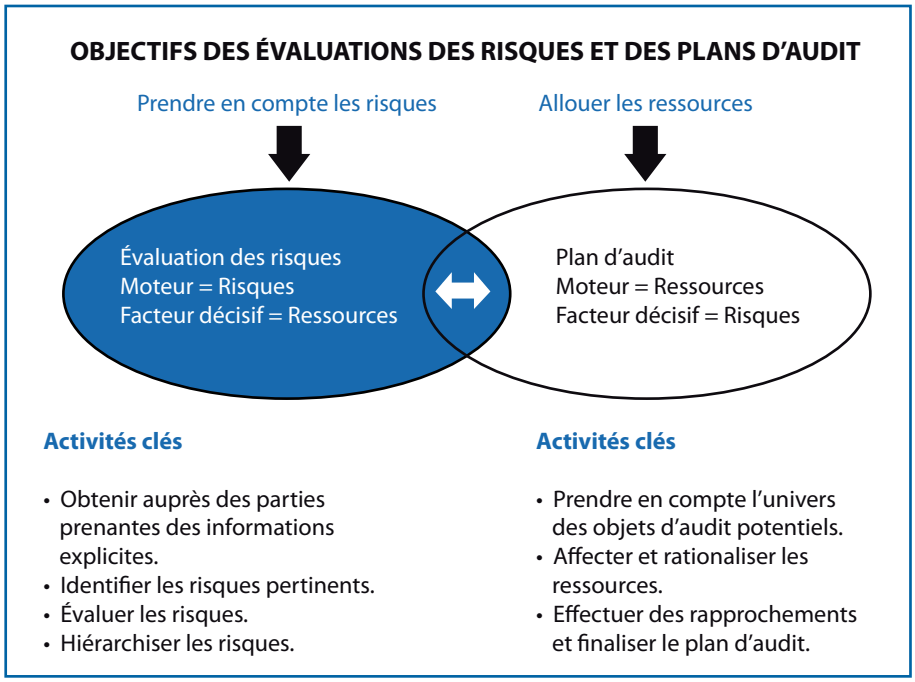

Figure 4. Objectifs des évaluations des risques et des plans d'audit (source : Ernst & Young, 2007).

- **Norme 2020 – Communication et approbation.** Le responsable de l'audit interne doit soumettre à la direction générale et à l'organe délibérant son programme d'audit et ses besoins, ainsi que tout changement important susceptible d'intervenir en cours d'exercice. Le responsable de l'audit interne doit également signaler l'impact de toute limitation de ses ressources.
- **Norme 2030 – Gestion des ressources.** Le responsable de l'audit interne doit veiller à ce que les ressources affectées à cette activité soient adéquates, suffisantes et mises en œuvre de manière efficace pour réaliser le programme d'audit approuvé.

6.2 Demandes des parties prenantes

Tout au long de l'élaboration du programme d'audit des SI, les auditeurs internes devront discuter avec les principales parties prenantes afin de mieux prendre en compte l'activité et les risques de l'organisation. Ces discussions leur permettront de rassembler des informations sur l'organisation, ainsi que sur les éventuelles préoccupations exprimées par ces parties prenantes. C'est aussi l'occasion de prendre connaissance des demandes spécifiques de missions de conseil et d'assurance, adressées à l'audit et appelées ci-après « demandes des parties prenantes ».

Les demandes des parties prenantes peuvent émaner du Conseil d'administration, du comité d'audit, des cadres dirigeants ou des responsables d'exploitation. Elles doivent être prises en compte au cours de la phase de planification de l'audit, en fonction de la capacité de la mission à améliorer le management global des risques et l'environnement de contrôle de l'organisation. Il se peut que ces demandes soient suffisamment précises pour que l'on puisse déterminer l'allocation des ressources nécessaires, ou que l'allocation des ressources se fonde sur les travaux d'audit précédents. Ces missions peuvent également comporter des enquêtes sur des soupçons de fraude qui peuvent survenir de manière inopinée et des demandes d'examen des activités de prestataires de services (la Norme 2010.C1 « Intégration des mission de conseil dans le plan d'audit » donne des informations sur la mission de conseil). Il faut donc que les responsables de l'audit interne envisagent d'accepter des projets de missions de conseil en se fondant sur la capacité de ces missions à améliorer le management des risques, à ajouter de la valeur à la réalisation des opérations de l'organisation et à en améliorer les conditions. Les missions acceptées seront intégrées dans le programme d'audit des SI.

6.3 Fréquence des audits

En fonction des résultats de l'évaluation des risques, tous les domaines ne peuvent pas ou ne devront pas être examinés dans chacun des cycles d'audit. Comme l'indique le chapitre 5, la fréquence des audits est définie sur la base d'une évaluation de la probabilité d'occurrence et de l'impact des risques en regard des objectifs de l'organisation. Les audits étant cycliques, des programmes d'audit pluriannuels sont élaborés et présentés à la direction générale et au comité d'audit, pour examen et validation. On élabore un plan pluriannuel, qui s'étend généralement sur trois à cinq ans, pour spécifier quels audits seront menés et quand, pour veiller à l'étendue adéquate des travaux effectués sur cette période et pour identifier les audits pouvant nécessiter des ressources externes spécialisées, voire des ressources internes supplémentaires. De surcroît, la plupart des organisations établissent un programme sur un an, qui découle du plan pluriannuel. Elles y énoncent les activités d'audit planifiées pour l'année à venir.

Les auditeurs peuvent recourir à l'une des deux stratégies suivantes pour déterminer la fréquence idéale des activités d'audit planifiées[13]:

- La fréquence des audits est déterminée d'après une évaluation initiale des risques, tous les trois à cinq ans, et elle est proportionnée au niveau de risque.
- Le plan d'audit s'appuie sur une évaluation des risques en continu, sans qu'une fréquence des audits ne soit prédéfinie. Certaines organisations appliquent

[13] *Brink's Modern Internal Auditing*, 6e édition, 2005, p. 292.

	Priorité	Fréquence	Allocation des ressources
É	Action immédiate généralement dans la première année	Examens annuels ou actions multiples durant le cycle d'audit	Allocation substantielle
M	Action à moyen terme durant le cycle d'audit	Une ou plusieurs missions d'audit durant le cycle d'audit peuvent être différées	Allocation de base
F	Missions généralement non planifiées durant le cycle d'audit	Au maximum une mission planifiée dans le cycle d'audit	Allocation limitée

Tableau 5. Fréquence des audits et allocation des ressources nécessaires

cette méthode, qui est particulièrement appropriée dans le contexte du plan d'audit des SI, étant donné que les SI évoluent plus rapidement que d'autres domaines.

Le tableau 5 présente des critères qui peuvent servir à déterminer la fréquence et l'allocation des ressources en fonction des résultats de l'évaluation des risques. Ce processus doit être compris comme une séquence d'activités, cyclique, répétitive et itérative, comportant une approche descendante avec au moins trois niveaux :

- Niveau 1, l'univers d'audit où toutes les données d'entrée sont intégrées.
- Niveau 2, les différents processus de l'organisation où il convient d'identifier et de planifier, au préalable, les missions d'audit.
- Niveau 3, les missions d'audit où l'on peut affiner et optimiser le plan.

Outre la fréquence des audits, l'élaboration du programme d'audit prendra en compte d'autres facteurs :

- **Stratégies de sous-traitance de l'audit interne.** Il est courant de mettre en œuvre différentes stratégies d'externalisation ou d'accroissement des effectifs, notamment l'embauche de personnel interne, l'externalisation et le co-sourcing, qu'il faut envisager au cours du processus de planification annuelle.
- **Estimation des ressources disponibles pour l'audit des SI.** Il s'agit d'inventorier les compétences techniques disponibles et d'en rapprocher les résultats avec les besoins d'audit des SI. La disponibilité des ressources est généralement déterminée sur une base annuelle et repose à la fois sur le nombre d'auditeurs ETP (équivalent temps plein) et sur les compétences nécessaires. Les jours d'audit disponibles correspondent à la différence entre le nombre de jours d'audit, fonction du potentiel nominal, et les activités non liées à l'audit ou les périodes non travaillées, telles que le temps de formation, les congés payés et les jours fériés.
- **Les demandes du Conseil d'administration et de la direction générale incluses dans le programme et portant sur le contrôle des services d'assurance et de conseil.**
- **L'obligation de se conformer à la réglementation et aux autres dispositions en vigueur.** Cette obligation sera incluse dans l'univers d'audit et dans l'évaluation des risques.
- **Les audits externes à synchroniser avec le plan d'audit.** La Norme de fonctionnement 2050 « Coordination » indique : « *Afin d'assurer une couverture adéquate et d'éviter les doubles emplois, le responsable de l'audit interne devrait partager des informations et coordonner ses activités avec les autres prestataires internes et externes d'assurance et de conseil.* »
- **Les initiatives et efforts internes destinés à améliorer la fonction d'audit.** Tout ce qui va au-delà des missions d'audit et constitue un investissement a besoin d'être planifié, budgétisé et présenté dans le plan d'audit. Exemples : revue de l'assurance qualité, évaluation intégrée des risques, communication au comité d'audit, suites données aux recommandations de l'audit.
- La mise en réserve **d'un budget et d'un programme d'audit des SI, permettant de faire raisonnablement face à des situations non prévues.**

6.4 Principes relatifs au plan d'audit

Lorsque les auditeurs internes définissent les principes relatifs au plan d'audit, ils doivent prendre en compte la MPA 2010-1 – La prise en compte des risques et des menaces pour l'élaboration du plan d'audit :

« 1. *En élaborant le plan d'audit interne, la plupart des responsables de l'audit interne choisissent d'abord de développer ou d'actualiser l'univers d'audit,* c'est-à-dire *une liste de tous les audits pouvant être réalisés. […]*

2. *L'univers d'audit peut intégrer certaines composantes du plan stratégique de l'organisation, […]* afin de *refléter les objectifs globaux […] et l'attitude de l'organisation face au risque et le degré de difficulté que comporte la réalisation des objectifs fixés. […]*
3. *Le responsable de l'audit interne prépare le plan d'audit interne à partir de l'univers d'audit, des contributions de la direction générale et du Conseil, d'une évaluation des risques et des menaces pouvant affecter l'organisation. […]*
4. *L'univers et la planification d'audit sont mis actualisés afin d'intégrer les changements d'orientation, d'objectifs et de priorité décidés par la direction générale […], au minimum une fois par an. […]*
5. *Le plan des missions d'audit est établi, entre autres, sur la base d'une évaluation des principaux risques et menaces. Il convient de définir des priorités de façon à affecter les ressources,* et il existe divers modèles de risques pour aider le responsable de l'audit interne dans cette tâche. […] »

6.5 Le contenu du programme d'audit des SI

Le contenu du programme d'audit des SI reflétera directement l'évaluation des risques décrite dans les sections

précédentes. Le plan présentera également différents types d'audit des SI, par exemple les suivants :

- Audits intégrés des processus de l'organisation.
- Audits des processus SI (audits de la stratégie et de la gouvernance des SI, audits des efforts déployés pour la gestion des projets, activités, politiques et procédures de développement des logiciels, processus COBIT/ISO/ITIL et sécurité de l'information, gestion des incidents, gestion des changements, gestion des patchs et assistance).
- Audits des projets de l'organisation et des initiatives portant sur les SI, notamment les revues du cycle de développement des logiciels.
- Revues au titre des contrôles applicatifs.
- Audits de l'infrastructure technique (revues de la gestion de la demande, évaluations de la performance, évaluations des bases de données, audits des systèmes d'exploitation, analyses des opérations, etc.).
- Audit du réseau (examen de l'architecture du réseau, tests d'intrusion, évaluation des vulnérabilités et de la performance).

Afin de vérifier que l'étendue de chaque audit est adéquate, les auditeurs peuvent se pencher sur les aspects suivants :

- Contrôles généraux des SI, contrôles applicatifs et contrôles de l'infrastructure.
- Contributions aux revues opérationnelles, aux revues des aspects financiers et aux examens de conformité.
- Principaux objectifs des contrôles (séparation des tâches, concentration des tâches et sécurité, entre autres).
- Nouvelles tendances des SI et menaces induites, innovations et impact.
- Toutes les couches SI.

6.6 Intégration du programme d'audit des SI

L'un des volets essentiels du processus de planification est la définition du degré d'intégration du plan d'audit des SI aux autres activités du service d'audit. Comme l'explique le paragraphe 4.7, les auditeurs déterminent quelle entité d'audit sera chargée de planifier et de surveiller les audits des applications métier. Cette analyse pourrait être élargie à toutes les composantes des SI. Par exemple, le plan d'audit des SI sera-t-il présenté et exécuté de manière autonome ou des objets d'audit liés aux SI seront-ils intégrés à d'autres domaines de l'organisation ? Pour répondre à cette question, il faut prendre en compte la fonction d'audit interne, ainsi que le personnel, la taille, la répartition géographique et le mode de management de ce service. On pourrait ainsi examiner divers scenarii d'intégration, allant d'un scénario de faible intégration, dans lequel la fonction d'audit des SI est bien définie et établie au sein du service d'audit interne (avec un univers et une étendue qui lui sont propres) à un scénario d'audit entièrement intégré, où toutes les composantes des SI sont bien prises en compte, pour chaque segment de l'organisation.

Le tableau 6 illustre des scenarii reposant sur différentes options d'intégration du plan d'audit des SI :

- **Un plan d'audit faiblement intégré.** Il s'agit d'un plan autonome d'audit des SI, placé sous la responsabilité de l'équipe d'audit des SI. Un plan faiblement intégré est organisé par domaines associés aux SI, généralement séparé des activités non liées à l'audit des SI et inclut la revue des applications. Le plus souvent, le champ de ces autres activités n'englobe aucune des composantes des SI.
- **Un plan d'audit partiellement intégré, énonçant les missions d'audit des SI définies par une équipe centrale d'audit des SI.** Ce type de plan comporte un ensemble supplémentaire de missions planifiées, que l'on appelle habituellement des revues d'applications et qui sont réparties entre d'autres équipes d'audit non spécialisées dans les SI et coordonnées avec les revues d'autres processus de l'organisation.
- **Un plan d'audit fortement intégré, dans lequel les activités d'audit des SI font partie intégrante des missions portant sur les processus de l'organisation.** Souvent, les activités d'audit des SI sont planifiées sous la responsabilité d'une équipe pluridisciplinaire dont les membres disposent d'un ensemble équilibré de compétences, notamment d'un savoir-faire en audit des SI.

Étant donné qu'un système de contrôle interne comporte généralement des contrôles manuels et des contrôles automatisés, avec un recours accru aux contrôles applicatifs, la capacité de définir l'étendue de l'audit de façon à prendre en compte tous les contrôles est essentielle pour une évaluation globale de l'environnement de contrôle. Un audit complet, incluant une revue de tous les éléments des SI, offre l'opportunité d'évaluer si la combinaison des contrôles permet de réduire les risques de l'organisation.

6.7 Validation du programme d'audit

Il n'existe malheureusement pas de test direct permettant de vérifier que le plan d'audit est adéquat et son efficacité potentielle maximale. Les auditeurs devront donc disposer de critères pour évaluer l'efficience de ce plan en regard de ses objectifs. Comme nous l'avons vu précédemment, le plan d'audit inclura les audits fondés sur le risque,

les domaines d'audit obligatoires et les demandes de la direction générale relatives à des activités d'assurance et de conseil. L'un des objectifs de la phase de planification étant d'allouer des ressources aux domaines dans lesquels l'audit interne peut créer le plus de valeur ajoutée, comme aux domaines des SI induisant le plus de risques, les auditeurs détermineront la manière dont le programme pourra refléter cet objectif.

La figure 5 (p.24) illustre ce à quoi aspirera l'audit. D'après ce schéma, étant donné que tous les objets et missions d'audit sont représentés en fonction de la probabilité et de l'impact des risques qui y sont associés, l'ensemble des quadrants du schéma reflètent tous les audits possibles. Dans les cases en gris, on trouve la sélection idéale d'audits et de missions : le programme d'audit se compose majoritairement des audits correspondant au quadrant du schéma rassemblant les risques les plus élevés, et les autres audits sont sélectionnés, de façon proportionnelle, dans les quadrants du schéma qui correspondent à un risque moyen ou faible. De plus, une partie des audits porteront sur la conformité et sur les domaines d'audit obligatoire. Par conséquent, les auditeurs noteront que, même s'il existe des raisons valables d'inclure dans le plan des audits associés à un risque faible, il convient d'envisager d'autres stratégies d'audit, telles que l'auto-évaluation des contrôles, afin de limiter les ressources nécessaires à la revue.

6.8 La nature dynamique du programme d'audit des SI

La technologie ne cessant d'évoluer, l'organisation se retrouve confrontée à de nouveaux risques, vulnérabilités et menaces. De surcroît, les changements technologiques peuvent amener à définir un nouvel ensemble d'objectifs pour les SI, ce qui débouche sur de nouvelles initiatives, acquisitions ou transformations dans le domaine des SI, ou des changements visant à répondre aux besoins de l'organisation. Lors de l'élaboration du plan d'audit, il importe donc de prendre en considération le caractère dynamique et évolutif de l'organisation. Plus précisément, les auditeurs devront alors tenir compte du rythme de changement des SI, plus rapide que celui des autres activités, de l'adéquation du calendrier de développement d'un système avec le résultat des audits de ce cycle de développement.

Les auditeurs tiendront compte de l'origine spécifique du changement. Ainsi, le plan d'audit des SI pourrait être révisé en raison des phénomènes suivants :

- Évolution des ressources stratégiques, organisationnelles ou humaines.
- Nouvelles initiatives portant sur les processus de l'organisation, notamment l'utilisation d'une technologie à haut risque, telle que le commerce électronique.
- Changements majeurs dans les applications : par exemple, adoption d'une nouvelle version d'une application de commerce en ligne.
- Adoption de suites logicielles de support et d'administration présentant un caractère critique.
- Menaces sur le réseau et sur les infrastructures, qui imposent de réévaluer la gestion de la sécurité de l'information.

En conséquence, il faut périodiquement réexaminer les priorités du programme d'audit des SI et, au besoin, en rendre compte au Conseil d'administration et à la direction générale plus fréquemment que pour d'autres domaines d'audit plus classiques et plus statiques. L'audit des SI devra

Univers d'audit	Plan d'audit faiblement intégré	Plan d'audit partiellement intégré	Plan d'audit fortement intégré
Processus • Opérationnels • Financiers • Conformité	Audit ne portant pas sur les SI	Audit ne portant pas sur les SI	Approche intégrée
Systèmes applicatifs • Contrôles applicatifs • Contrôles généraux des SI	Audit des SI	Approche intégrée	Approche intégrée
Contrôles de l'infrastructure SI • Bases de données • Systèmes d'exploitation • Réseau	Audit des SI	Audit des SI	Approche intégrée

Tableau 6. Audit des SI et audit intégré

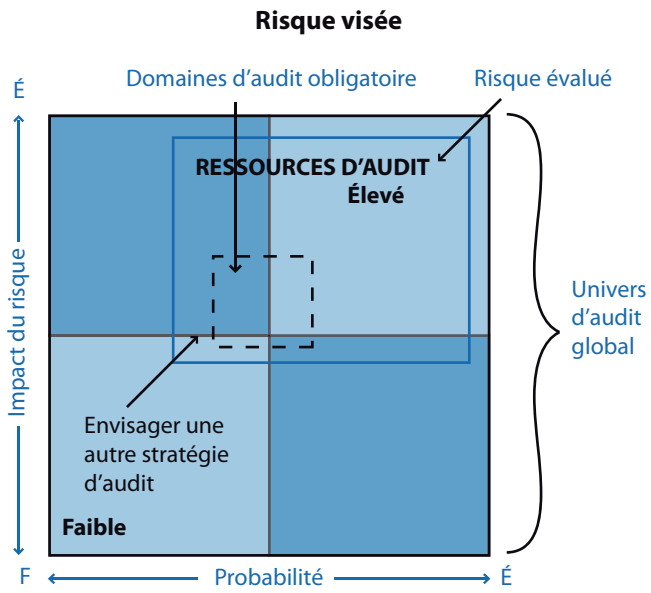

Figure 5. Résultats d'audit visés.

également analyser les changements de l'univers d'audit des SI et se montrer suffisamment souple pour adapter son programme aux nouvelles situations. De surcroît, il convient de réévaluer le plan périodiquement et de faire montre d'une plus grande flexibilité pour réagir aux évolutions de l'activité et des environnements de SI en ajustant le classement et l'ordre de priorité des audits planifiés. Enfin, il est essentiel que le plan mette en relation chaque élément de l'univers d'audit des SI avec l'une des phases suivantes du cycle de développement des logiciels : étude de faisabilité, analyse, conception, implémentation, tests, évaluation, maintenance et production.

La valeur ajoutée apportée par une fonction d'audit interne dépend largement de la qualité des recommandations de cette fonction et des effets positifs que l'organisation peut retirer de leur mise en œuvre. Ainsi, il est souvent directement bénéfique de remédier aux problèmes de conformité liées aux règles financières/monétaires. En revanche, il peut être indirectement bénéfique de contribuer à améliorer la réputation, l'avantage concurrentiel, la maturité des processus et la capacité d'innovation d'une organisation.

Le facteur temporel est l'une des principales caractéristiques des recommandations de l'audit qui influent sur la valeur ajoutée. Il est important durant tout le cycle des applications des SI. En général, plus on identifie tôt une faiblesse ou un risque dans le cycle de vie des logiciels, plus les recommandations de l'audit créeront de la valeur ajoutée. Ainsi, le coût de mise en œuvre d'une modification majeure destinée à remédier à la faiblesse d'une application critique est nettement plus élevé quand le système est en production que lorsque la même faiblesse est traitée au cours de la phase de conception.

Outre la valeur ajoutée qui découle de la qualité des recommandations de l'audit, le professionnalisme de l'auditeur interne s'en trouve davantage reconnu. La fonction d'audit interne déterminera ensuite comment planifier ses travaux pour formuler le bon type de recommandations dans un délai optimal par rapport à la durée du cycle de développement En principe, la stratégie de planification sera déployée avant le début du cycle, afin que des actions appropriées puissent être planifiées en termes de temps et de ressources.

Il est impératif que le plan d'audit des SI parvienne à équilibrer les travaux d'audit sur l'ensemble du cycle, de façon à éviter la concentration des efforts sur la phase de maintenance et de production, et à délimiter un champ d'audit adéquat durant les phases initiales. En suivant ces recommandations, les organisations pourront passer d'une stratégie classique de planification traditionnelle et *a posteriori* (c'est-à-dire reposant principalement sur les activités opérationnelles, la conformité et les aspects financiers) à une approche plus innovante, source de valeur ajoutée et par nature plus consultative.

6.9 Communiquer, obtenir le soutien de la direction et faire approuver le programme d'audit

Le service d'audit interne présente le programme d'audit à la direction générale et au comité d'audit. D'après la Norme 2020, il doit, en particulier, informer ces instances du niveau de ressources requis, de tous les remplacements significatifs susceptibles d'intervenir en cours d'exercice et de l'impact potentiel d'une limitation de ses ressources[14].

Il importe également que le volet SI du programme d'audit interne ou que le programme d'audit du SI fasse l'objet d'une discussion avec la direction générale et l'organe délibérant, ainsi qu'avec les principaux acteurs impliqués à travers le SI, telles que le DSI, les directeurs de la production et des développements, les cadres de la DSI, les propriétaires d'application et d'autres membres du personnel exerçant des fonctions analogues. La contribution de ces parties prenantes est cruciale pour le succès de la planification de l'audit comme devant permettre aux responsables de l'audit interne et aux auditeurs internes de mieux cerner l'environnement de l'organisation, d'identifier les risques et les préoccupations et de sélectionner les domaines d'audit. De plus, le dialogue sur le programme d'audit définitif aidera à valider la contribution des parties prenantes tout au long du processus et donnera un premier aperçu des travaux à mener.

Les auditeurs discutent du plan d'audit des SI avec les principaux responsables, les gestionnaires et le personnel

[14] *Internal Auditing: Assurance & Consulting Services* (2007), Kurt F. Reding *et al.*, ISBN 978-0-89413-610-8, p. 8-11.

chargé des SI de façon à obtenir leur soutien. La compréhension, la coordination et le soutien de l'équipe chargée des SI rendront le processus d'audit plus efficace et plus efficient. De plus, la connaissance anticipée du programme facilite un dialogue franc et permanent, qui permet de discuter de l'évolution des risques et de l'environnement opérationnel, à chaque étape de la réalisation du plan d'audit, et de procéder à des ajustements en continu. L'interaction avec les « clients » lors de l'évaluation des risques et avant l'approbation du plan d'audit final est fondamentale pour la qualité globale du plan.

7. Annexe : Exemple d'une entreprise fictive

L'exemple présenté dans ce chapitre illustre la façon d'intégrer les éléments servant à planifier l'audit des SI, qui sont analysés dans les sections précédentes. Il s'agit d'étapes qui peuvent être universellement suivies, mais, dans cet exemple, les objets d'audit et les résultats de l'évaluation des risques revêtent un caractère général.

7.1 L'entreprise

Notre entreprise fictive est cotée en Bourse. Elle produit et fournit des matières premières mises en œuvre par des fabricants de biens de consommation sur différents marchés dans le monde. Voici son profil :

- Total des actifs : 7 milliards de dollars.
- Société basée aux États-Unis.
- Trente sites de production dans sept pays : Arabie saoudite, Belgique, Chine, Corée du Sud, États-Unis, Qatar et Singapour.
- Six centres de recherche, de technologie et de contrôle de la qualité, sur chaque site de production.
- Cinq mille salariés dans le monde.
- Cinq grands concurrents.
- Près de 3 000 brevets nationaux et internationaux et demandes de brevet.
- Trois principales directions opérationnelles pour la fabrication des différentes lignes de produits, siège centralisé et entités fournissant des services support.
- Trois gros projets d'investissement destinés à renforcer et étoffer la capacité de production.

De plus, l'organisation centralisée des SI de cette entreprise comporte quatre divisions de base :

- Infrastructure globale :
  - Télécommunications.
  - Communications vocales.
  - Réseaux.
  - Connexion à distance.
  - Informatique de bureau et Internet.
  - Gestion du cycle de vie de l'information.
  - Serveurs.

- Applications d'entreprise :
  - Une grande application ERP utilisée dans toute l'entreprise pour la gestion de la chaîne logistique, la comptabilité générale, les ressources humaines (basées aux États-Unis), la vente et la distribution.
  - Support technique SAP et programmation ABAP (*Advanced Business Application Programming*).

- Systèmes de production :
  - Responsable des systèmes utilisés sur les sites de production.
  - Applications locales, incluant la gestion de la paie pour les sites hors États-Unis, les bases de données pour la recherche et le contrôle de la qualité, le reporting environnemental et les systèmes de contrôle des processus de production.
  - Analyse financière et contrôles financiers.

- Stratégie et gestion des risques :
  - Contrats, achats et licences.
  - Stratégie, architecture et normes.
  - Services de sécurité.
  - Changement au niveau des SI et gouvernance des SI.
  - Bureau de gestion des projets.

Les sites de production forment le cœur de l'organisation. Étant disséminés à travers le monde et n'ayant pas tous la même capacité, ils induisent des risques susceptibles d'influer sur les fondamentaux et sur les aspects financiers de l'entreprise. Qui plus est, même si ces sites de production constituent un modèle d'entreprise légèrement décentralisé, la composante globale et les composantes de service centralisées offrent l'opportunité de réaliser des audits axés sur les processus dans plusieurs fonctions de l'entreprise à la fois.

En ce qui concerne la conformité, l'organisation relève de la législation des États-Unis et de la législation européenne, notamment de la loi Sarbanes-Oxley, de la directive européenne sur la protection des données à caractère personnel, du *Foreign Corrupt Practices Act* (États-Unis) et d'autres dispositions applicables aux sites sur lesquels elle opère. D'après son plan d'activité (business plan) annuel, l'entreprise a plusieurs grands projets d'investissement en cours qui auront un impact considérable sur sa compétitivité à venir.

Enfin, la fonction SI est bien harmonisée avec le *modèle d'activité*. Cette société utilise un groupe d'applications relativement homogène, dont une application ERP standard, une infrastructure globale de serveurs et de réseaux, ainsi que des processus d'appui standard pour la mise à disposition de services de SI, la gouvernance et la sécurité.

7.2 Le plan d'audit des SI

La description ci-dessus permet d'identifier un univers d'audit des SI dont découle une liste générale des domaines d'audit envisageables et qui informe la direction sur l'efficacité de l'environnement de contrôle et des opérations de l'entreprise.

Comme indiqué dans les paragraphes précédents, la composante globale et les composantes de service centralisées offrent l'opportunité de définir des objets d'audit globaux axés sur les processus. L'application ERP centralisée, les domaines support de l'infrastructure globale et les processus standard mettant à disposition des prestations informatisées sont de bons « candidats » pour des objets d'audit indépendants, couvrant de larges pans du risque associé aux SI.

Les sites de production sont également représentés dans l'univers d'audit des SI par des objets d'audit faisant partie d'applications supportées localement et par une infrastructure sous-jacente (notée, pour simplifier, « site 1-30 » dans le tableau 7). Ces objets d'audit sont susceptibles de correspondre aux audits des processus, sur chaque site.

Le tableau 7 présente un exemple d'univers d'audit constitué de thèmes d'audit des SI envisageables pour l'entreprise. On trouve ces objets d'audit, et d'autres, dans chacun des 30 sites de production.

Directions métiers	Sujet d'audit
Composante globale	Administration et sécurité du réseau
Composante globale	Connexion à distance
Composante globale	Administration et sécurité des serveurs sous Windows
Composante globale	Administration et sécurité sous UNIX
Composante globale	Contrôles de l'application ERP et contrôles généraux
Composante globale	Revue de la conformité à la loi Sarbanes-Oxley
Composante globale	Respect de la politique de confidentialité de l'entreprise
Composante globale	Administration et sécurité des bases de données
Composante globale	Pratiques de gouvernance des SI
Composante globale	Pratiques de déploiement de l'ITIL
Composante globale	Contrôle des changements apportés aux programmes applicatifs
Segment d'activité 1-3	Grands projets d'investissement (protection de l'information et conformité de l'entreprise, notamment)
Site 1-30	Infrastructure SI
Site 1-30	Application RH/paie
Site 1-30	Systèmes de contrôle des processus

Tableau 7. L'univers d'audit des SI

Après avoir défini l'univers d'audit des SI à un niveau élevé, il faut ensuite évaluer les risques de l'entreprise et les risques associés aux SI dans chaque domaine. Les catégories de risques sont évaluées d'après leur probabilité d'occurrence et l'impact qu'elles auraient sur l'organisation si le management des risques n'était pas approprié. Cette approche fondée sur les risques recourt à un classement relatif (tableau 8). On peut, par exemple, utiliser une échelle de notation à trois degrés pour l'évaluation de la probabilité et de l'impact :

Échelle de probabilité		
É	3	Probabilité élevée que le risque survienne
M	2	Probabilité moyenne que le risque survienne
F	1	Faible probabilité que le risque survienne

Échelle d'impact (financier)		
É	3	Impact potentiel important sur le résultat, les actifs, la réputation ou les parties prenantes de l'organisation.
M	2	L'impact potentiel peut être significatif pour l'unité auditée, mais modéré pour l'organisation dans son ensemble.
F	1	L'impact potentiel sur l'organisation est minime ou d'ampleur limitée.

Tableau 8. Échelle de notation à trois degrés pour l'évaluation de la probabilité et de l'impact

Pour faciliter l'analyse, on sélectionne une fourchette indiquant le niveau de risque (élevé, moyen ou faible) :

Niveau	Fourchette des scores composites du risque	Fréquence recommandée pour le cycle d'audit
É	35-54	Tous les ans ou tous les 2 ans
M	20-34	Tous les 2 à 3 ans
F	6-19	Tous les 3 à 5 ans

Tableau 9. Niveau de risque

Pendant la phase d'évaluation des risques, les auditeurs ont à définir une fréquence recommandée pour l'examen des objets d'audit qui font partie de l'univers d'audit, en fonc-

tion de la fourchette des scores composites du risque : les objets d'audit à risque élevé seront examinés tous les ans ou tous les deux ans, les sujets à risque moyen tous les deux à trois ans, et les sujets à risque faible tous les trois à cinq ans. Les domaines à risque élevé pourront ainsi être examinés fréquemment et ceux à risque faible couverts de manière

Domaine	Impact financier		Risques liés aux SI										Score et niveau	
			Qualité du dispositif de contrôle interne		Changements dans l'unité d'audit		Disponibilité		Intégrité		Confidentialité			
	P	I	P	I	P	I	P	I	P	I	P	I		
Contrôles de l'application ERP et contrôles généraux	3	3	2	3	3	3	2	3	2	3	2	3	42	É
Systèmes de transfert électronique de fonds	3	3	3	3	3	3	3	2	3	2	2	1	41	É
Site 3 - Applications RH/paie	3	3	3	2	3	3	2	2	2	3	2	3	40	É
Applications relatives aux avantages sociaux (externalisées)	2	3	2	2	3	3	3	2	2	3	3	3	40	É
Site 3 - Infrastructure SI	2	2	3	2	3	3	3	3	3	2	2	2	38	É
Site 3 - Systèmes de contrôle des processus	3	3	3	2	3	3	3	3	2	2	2	1	39	É
Administration et sécurité sous UNIX	2	2	3	2	3	3	2	3	3	2	2	2	35	M/É
Respect de la politique de confidentialité de l'entreprise	3	1	3	3	3	3	2	1	2	1	3	3	34	M/É
Administration et sécurité des bases de données	2	2	2	2	2	2	3	3	2	2	2	1	27	M
Administration et sécurité des serveurs sous Windows	2	2	1	2	2	2	2	3	3	2	2	2	26	M
Site 1 - Infrastructure SI	2	2	3	2	1	3	3	2	3	1	1	1	23	M
Site 1 - Systèmes de contrôle des processus	2	3	3	2	2	2	3	3	1	1	1	1	27	M
Systèmes de reporting environnemental	2	2	3	2	2	2	2	3	1	1	3	1	24	M
Site 2 – Infrastructure SI	2	2	3	2	1	3	3	2	3	1	1	1	23	M
Grands projets d'investissement	2	2	3	3	1	1	2	2	1	1	2	3	25	M
Contrôle des changements apportés aux programmes applicatifs	2	3	2	3	1	2	2	2	1	3	1	2	23	M
Examen de la conformité à la loi SOX	2	2	2	3	2	2	1	2	2	2	1	2	22	M

Domaine	Impact financier		Risques liés aux SI										Score et niveau	
			Qualité du dispositif de contrôle interne		Changements dans l'unité d'audit		Disponibilité		Intégrité		Confidentialité			
	P	I	P	I	P	I	P	I	P	I	P	I		
Administration et sécurité du réseau	2	2	2	1	2	2	2	2	2	2	2	2	22	**M**
Site 2 - Systèmes de contrôle des processus	2	2	2	2	1	2	2	2	2	2	1	1	19	**M/F**
Pratiques de déploiement de l'ITIL	1	2	2	3	3	1	3	1	1	3	2	1	19	**M/F**
Site 2 - Applications RH/paie	1	2	1	2	2	3	2	2	3	1	1	2	19	**M/F**
Site 30 - Applications RH/paie	1	1	1	2	2	2	2	2	2	2	1	2	17	**F**
Site 1 - Applications RH/paie	1	1	1	2	2	2	2	2	2	2	1	1	17	**F**
Site 30 – Infrastructure SI	1	1	3	1	1	1	2	2	2	1	1	1	12	**F**
Site 30 - Systèmes de contrôle des processus	1	1	2	2	2	2	2	2	1	1	1	1	15	**F**
Pratiques de gouvernance des SI	1	1	2	2	1	1	3	1	1	1	1	2	12	**F**
Connectivité à distance	1	1	1	2	2	1	1	1	1	2	2	2	12	**F**

P = Probabilité
I = Impact

Tableau 10. L'analyse de risque

adéquate tous les trois à cinq ans. Le tableau 10, page 28, donne un exemple des résultats d'une analyse de risques.

Lorsque les résultats de l'analyse de risques sont disponibles, l'étape suivante consiste à formaliser le plan d'audit. Comme indiqué dans le chapitre 6, le programme d'audit se compose de projets d'audit fondés sur les risques, d'examens obligatoires de la conformité, de demandes des parties prenantes et d'audits de suivi des problèmes significatifs déjà identifiés. Ces tâches devant être réalisées avec les ressources d'audit interne disponibles, il se peut que certains projets d'audit axé sur les risques ne soient pas intégrés dans le plan d'audit.

Poursuivons notre exemple d'entreprise fictive : le Conseil d'administration de cette entreprise a demandé au service d'audit des SI de prendre part à la coordination d'un test d'intrusion sur une infrastructure externe, et les responsables de l'exploitation ont souhaité obtenir l'assurance que la conformité du management à la loi Sarbanes-Oxley était examinée dans toute l'organisation. De plus, la DSI a demandé au service d'audit interne de participer au projet de déploiement de l'ITIL afin de déterminer si les processus de prestation de services étaient efficaces et couvraient tous les risques.

Ces demandes émanant de tierces parties sont acceptées parce qu'elles entrent dans le cadre de la mission du service d'audit interne, et elles seront automatiquement intégrées au programme d'audit. En outre, l'audit des processus d'achat, réalisé l'année précédente, ayant fait apparaître un important problème concernant la séparation des tâches, un audit de suivi sera ajouté dans le plan d'audit afin de veiller à ce que les actions correctives progressent comme prévu. Enfin, la conformité de la nouvelle politique globale relative à la protection des données personnelles fera, elle aussi, partie du programme d'audit, car il existe des projets de transmission des données personnelles entre les sites hors États-Unis et le siège américain.

L'entreprise dispose d'une équipe de cinq auditeurs pour les SI, soit environ 1 000 jours disponibles pour les missions,

compte tenu des périodes non travaillées et de formation. Le tableau 11 présente le programme d'audit le plus efficace d'après l'évaluation des risques associés aux objets d'audit disponibles, aux domaines d'audit obligatoire et aux demandes des tierces parties. Plusieurs objets d'audit à risque élevé n'ont pas été inclus dans ce plan (notamment les systèmes de transfert électronique de fonds, les systèmes de contrôle des processus et l'administration et la sécurité des bases de données) parce qu'ils ont été examinés au cours des 12 derniers mois.

Mission	Niveau de risque	Cycle	Jours d'audit alloués
Coordination du test d'intrusion	*	0	40
Suivi de l'application relative aux achats	*	0	20
Contrôles de l'application ERP et contrôles généraux	É	1	100
Site 3 – Application RH/paie	É	2	30
Applications relatives aux avantages sociaux du personnel (externalisées)	É	3	100
Site 3 – Infrastructure SI	É	2	90
Administration et sécurité sous UNIX	M/É	1	90
Respect de la politique de confidentialité de l'entreprise	M/É	3	40
Administration et sécurité des serveurs sous Windows	M	3	90
Site 1 – Infrastructure SI	M	3	90
Site 1 – Systèmes de contrôle des processus	M	3	90
Systèmes de reporting environnemental	M	3	30
Grands projets d'investissement	M	3	30
Conformité à la loi Sarbanes-Oxley	M/*	3	120
Pratiques de déploiement de l'ITIL	F/*	4	40
Total			1000
* Demande de la direction			

Tableau 11. Le plan d'audit

Le plan d'audit présenté dans le tableau 11 constitue une perspective idéale, étant donné le profil du service d'audit interne, sa compréhension des stratégies et des objectifs de l'entreprise, sa connaissance de l'historique de l'environnement de contrôle et les changements devant intervenir dans les processus opératoires au cours de la campagne d'audit à venir. Le plan est examiné avec la direction générale et les responsables opérationnels, dans le cadre d'une discussion faisant suite aux phases d'évaluation des risques et de planification des audits. Cet examen permettra de vérifier que la contribution du management a été prise en compte de manière précise dans le processus et donnera aux managers un premier aperçu du programme d'audit des SI pour l'année à venir.

C'est aussi lors de cet examen qu'il convient de discuter des dates des missions d'audit potentielles, car l'entreprise est susceptible de connaître des périodes d'arrêt total en raison d'une possible interruption de ses opérations. Il faut, par exemple, discuter des dates prévues pour la mise en œuvre des extensions de l'infrastructure, ainsi que des calendriers relatifs aux activités opérationnelles les plus importantes, telles que les réorganisations ou les fermetures d'usines, qui pourraient influer sur le processus d'audit.

Une fois que le plan a été finalisé, la réalisation des audits et la mobilisation correspondante des ressources disponibles sont planifiés. Il faut généralement désigner des auditeurs disposant des compétences requises, afin d'assurer le succès de la mission. Cependant, la programmation des audits est aussi une bonne opportunité de répondre aux besoins de développement du personnel en menant des audits qui élargiront et étofferont tel ou tel domaine de compétence.

Enfin, étant donné la nature dynamique de l'organisation, certains changements pourraient influer sur le programme et le calendrier d'audit. C'est pourquoi, il est essentiel de mettre en place un plan efficace, de le gérer sur toute sa durée et de s'adapter aux mutations de l'entreprise, de façon à ce que les ressources restent axées sur les domaines présentant un risque et, même si ces domaines évoluent, sur les préoccupations de l'organisation.

Glossaire

Activités de conseil : Conseils et services y afférents convenus avec le client afin d'améliorer le gouvernement d'entreprise, le management des risques et l'environnement de contrôle d'une organisation.

Cadre de référence (référentiel) : Principes directeurs formant un modèle que les organisations peuvent utiliser pour évaluer leurs pratiques.

Code d'un programme applicatif : Ensemble de programmes informatiques, fichiers de contrôle, tables et interfaces utilisateur qui confèrent une fonctionnalité opérationnelle à des processus spécifiques, telles que la comptabilité, la paie ou les achats.

Conformité : Acceptation et respect de la législation et de la réglementation en vigueur, incluant également l'adhésion aux règles, plans, procédures, contrats et autres exigences.

Environnement de contrôle : positionnement de la direction générale et de l'encadrement en regard de l'importance qu'ils attachent au dispositif de contrôle de l'entreprise. L'environnement de contrôle constitue le cadre et la structure nécessaires à la réalisation des objectifs primordiaux du système de contrôle interne.

Évaluation des risques : Méthode visant à déterminer la probabilité d'occurrence d'un événement susceptible d'empêcher l'organisation d'atteindre ses buts et objectifs de manière efficace, efficiente et maîtrisée.

Fonction d'audit interne : Service, division, équipe de consultants ou autres intervenants menant, de manière objective et indépendante, des travaux d'évaluation et de conseil, destinées à créer de la valeur ajoutée et à améliorer les opérations d'une organisation.

Infrastructure SI : Composantes clés de l'infrastructure technique d'une application, notamment le code logique de ses programmes, la base de données, le système, le réseau et l'environnement physique de chaque composante.

Management des risques (gestion des risques) : Processus de management destiné à prendre en compte et traiter les incertitudes qui pourraient altérer la capacité de l'organisation à atteindre ses objectifs.

Normes : codification des processus où procédures en vigueur dans l'entreprise, dont l'application est obligatoire et qui donne des orientations sur la façon de se conformer à la politique à laquelle la norme est associée. Les normes relatives aux SI sont, en général, technologiquement neutres et peuvent être scindées en contrôles spécifiques aux SI et en directives générales.

Politique : Déclaration écrite indiquant l'intention, les objectifs, les exigences et les responsabilités du management.

Processus : Un ensemble d'activités de l'entreprise liées les unes aux autres en vue de la réalisation d'un objectif commun.

Progiciel de gestion intégré (*Enterprise resource planning* – ERP) : Grandes applications informatiques qui gèrent la totalité d'un processus Elles intègrent ainsi des activités comme celles relatives aux achats, aux stocks, à la vente, à la distribution, aux ressources humaines et au service client, ainsi qu'à la gestion financière et d'autres aspects organisationnels.

Projets de mise en place de systèmes : travaux à grande échelle réalisés au sein de la fonction de mise à disposition des SI, destinés à permettre le déploiement de nouveaux systèmes applicatifs ou éléments d'infrastructure. Ces travaux peuvent inclure, par exemple, des activités de gestion de projets, de réingénierie de processus, ou des techniques de gestion du changement.

Réseaux : Dispositifs matériels et logiciels, tels que commutateurs, routeurs, pare-feux, câblages, programmes, qui commandent le routage des paquets de données afin de mettre en relation des ordinateurs et de leur permettre de communiquer entre eux.

Responsable de l'audit interne : Au sein d'une organisation, poste hiérarchique le plus élevé en charge des structures d'audit interne.

Risque : Possibilité que se produise un événement (menace) qui aura un impact sur la réalisation des objectifs de l'entreprise. Le risque se mesure en termes d'impact (conséquences) et de probabilité d'occurrence.

Processus de services support : Dans le contexte des SI, processus permettant de gérer l'infrastructure SI, ainsi que le développement et l'installation de nouveaux systèmes informatiques et de nouveaux traitements opérationnels recourant aux SI. Ces processus incluent notamment les activités d'assistance et les procédures de gestion des configurations, des changements, des mises en production, des incidents et des problèmes.

Sous-traitance (externalisation) : Recours à un tiers pour fournir une prestation de services (a priori non stratégiques)

au profit de l'entreprise. La sous-traitance gagne en importance en raison du coût élevé et du savoir-faire nécessaires pour fournir ces services.

Systèmes de bases de données : Ensemble de programmes permettant le stockage, l'actualisation et l'extraction de données enregistrées sur un support informatique.

Système de contrôle interne : Système englobant les cinq composantes du contrôle interne, à savoir l'environnement de contrôle, l'évaluation des risques, les activités de contrôle, l'information et la communication, et le pilotage, afin que le risque soit maîtrisé.

Système d'exploitation : Logiciel exécutant les tâches élémentaires d'un ordinateur, notamment le traitement des données saisies par l'opérateur, la gestion de la mémoire interne de l'ordinateur ou celle des fonctionnalités de lecture de disque, d'affichage et de périphériques.

Tiers : Entité non affiliée à l'organisation, ou à une entité de l'organisation.

Liste des acronymes

CBOK : Common Body of Knowledge (Base commune de connaissance) de l'IIA Research Foundation.

COBIT : Control Objectives for Information and Related Technology.

COSO : Committee of Sponsoring Organizations of the Treadway Commission.

ERP : Enterprise resource planning (progiciel de gestion intégré).

GLBA : Gramm-Leach Bliley Act (loi des États-Unis).

GTAG : Guide pratique d'audit des technologies de l'information.

HIPAA : Health Insurance Portability and Accountability Act (loi des États-Unis).

IIA : The Institute of Internal Auditors.

ISO : Organisation internationale de normalisation.

ITGI : IT Governance Institute.

ITIL : IT Infrastructure Library (bibliothèque d'infrastructure des technologies informatiques) de l'Office du commerce britannique.

PCAOB : Public Company Accounting Oversight Board (États-Unis).

PCI DSS : Payment Card Industry Data Security Standard.

SI : Systèmes d'information.

SOX : Loi Sarbanes-Oxley de 2002.

UE : Union européenne.

À propos des auteurs

Kirk Rehage

Kirk Rehage est responsable de l'audit des SI chez Chevron Corp., membre de l'Advanced Technology Committee de l'IIA et de l'ISACA, et gouverneur temporaire du chapitre du Nord de la Californie - East Bay de l'IIA. En tant que responsable de groupe en audit des SI, Kirk Rehage est chargé des activités d'assurance du service d'audit interne dans le domaine des SI, ainsi que des activités de conseil, dans plus de 180 pays.

Kirk Rehage a plus de 30 ans d'expérience dans le secteur de l'énergie et a exercé une grande diversité de fonctions en relation avec la mise à disposition de services de SI, telles que la mise en place d'une infrastructure informatique et d'environnements de réseaux, la gestion d'organisations proposant des applications, la programmation technique de solutions logicielles analytiques et de bases de données en ingénierie et en sciences de la terre.

Steve Hunt, CIA, CISA, CBM

Steve Hunt est l'un des directeurs principaux du groupe de conseil en entreprise et gestion des risques Crowe Chizek and Company LLC, vice-président de l'Advanced Technology Committee de l'IIA et membre de l'ISACA ainsi que de l'Association of Professionals in Business Management. Chez Crowe Chizek, Steve Hunt travaille avec les entreprises *Fortune 1000* de taille moyenne opérant sur des marchés restreints dans divers secteurs. Il supervise l'exécution des missions de gestion des risques financiers, opérationnels et informatiques.

Steve Hunt compte plus de 20 ans d'expérience dans différents secteurs : comptabilité, audit interne et conseil en management. Il a notamment réalisé des audits détaillés de la conformité avec la loi Sarbanes-Oxley, ainsi que d'autres audits internes et externes, et participé à des projets de réingénierie des processus et à des initiatives de développement de l'entreprise. Il possède également plusieurs années d'expérience en configuration des applications SAP R/3 et des contrôles de la sécurité des applications et des processus opérationnels. Il a également donné des conférences spécialisées dans plusieurs universités et organisations aux États-Unis.

Fernando D. Nikitin, CIA, CISA, CGEIT, CISM, CISSP

Fernando Nikitin a plus de 16 ans d'expérience en audit interne, gouvernance des SI et sécurité de l'information. Il a travaillé pour le secteur bancaire, pour l'administration publique et pour des organisations multilatérales. Il travaille comme auditeur interne au sein de l'Office of the Auditor General de la Banque interaméricaine de développement. Il était auparavant directeur de l'audit des SI à la Banco de la República Oriental del Uruguay.

Fernando Nikitin est membre de l'Advanced Technology Committee de l'IIA, membre du Conseil du Government and Regulatory Agencies Board de l'ISACA et collaborateur du National Institute of Technology de l'Inde. Il a également été président du chapitre uruguayen de l'ISACA à Montevideo et il est co-fondateur du chapitre uruguayen du Project Management Institute et membre de l'International Information Systems Security Certification Consortium. Fernando Nikitin a obtenu un MBA à l'EOI Business School de Madrid, en Espagne.

Réviseurs

L'IIA tient à remercier les personnes et organisations suivantes pour leurs précieux commentaires et leurs apports à cet ouvrage :

- Professional Practices Committee :
  - Advanced Technology Committee.
  - Board of Regents.
  - Committee on Quality.
  - Internal Auditing Standards Board.
  - Professional Issues Committee.
  - Ethics Committee.

- Urton Anderson, McCombs School of Business, Université du Texas à Austin, États-Unis ;
- Lily Bi, IIA, États-Unis ;
- Larry Brown, The Options Clearing Corp., États-Unis ;
- Faisal R. Danka, Londres, Royaume-Uni ;
- Christopher Fox, ASA, eDelta, New York, États-Unis ;
- Nelson Gibbs, Deloitte & Touche LLP, États-Unis ;
- Frank Hallinan, Chevron Phillips Chemical Co. LP, États-Unis ;
- Greg Kent, SecureIT, États-Unis ;
- Lemuel Longwe, Ernst & Young Chartered Accountants, Zimbabwe ;

- Steve Mar, Resources Global, États-Unis ;
- Tom Margosian, Ford Motor Company, États-Unis ;
- James Reinhard, Simon Property Group Inc., États-Unis.

L'IFACI tient à remercier pour leurs précieux commentaires à la traduction de cet ouvrage :

- Dominique VAN EGROO, Directeur Associé, FINTOO ;
- Jean-Claude HILLION, Inspecteur Général Honoraire de la Banque de France.

Élaboration d'un plan d'audit des SI

Étant donné que les organisations s'appuient largement sur les SI, les responsables de l'audit interne ont impérativement à savoir élaborer un programme d'audit du SI et déterminer la fréquence et le niveau de détail de chaque mission. Or, plusieurs examens de l'évaluation externe de la qualité effectués par l'IIA révèlent que la conception d'un programme d'audit des SI approprié constitue l'un des points les plus faibles des structures d'audit interne. Dans de nombreux cas, les auditeurs internes limitent leurs investigations aux connaissances techniques dont ils disposent le reste étant sous-traité, laissant des tiers décider finalement ce qu'il faut auditer dans ce domaine.

Le présent guide consacré à l'élaboration du plan d'audit des SI peut donc aider les responsables de l'audit interne et les auditeurs internes à :

- acquérir une connaissance de l'entreprise ainsi que de l'apport du SI dans le traitement de ses opérations.
- définir et prendre en compte l'environnement de SI.
- tenir compte de l'importance des évaluations de risques dans la délimitation de l'univers d'audit des SI.
- formaliser le programme annuel d'audit des SI.

Ce guide prend aussi l'exemple d'une entreprise fictive afin de montrer aux responsables de l'audit interne et aux auditeurs internes comment suivre les étapes nécessaires pour définir l'univers d'audit des SI.

Pour attribuer une note à ce guide ou formuler des commentaires, veuillez vous rendre sur :

www.theiia.org/guidance/technology/gtag11.

GTAG®

The Institute of Internal Auditors