GTAG®

GLOBAL TECHNOLOGY AUDIT GUIDE

Les risques et les contrôles des systèmes d'information

2ème édition

The Institute of Internal Auditors

Contenu

Résumé 4

1. Introduction 5

2. Fondamentaux concernant les risques et les contrôles des SI 8
   2.1 Concepts clés 8
   2.2 Gouvernance des SI 9

3. Parties prenantes internes et responsabilités des SI 12

4. L'analyse des risques 14
   4.1 Prise en compte du risque dans l'évaluation de l'adéquation des contrôles des SI 14
      4.1.1 L'environnement des SI 15
      4.1.2 Les risques informatiques rencontrés par l'organisation 15
      4.1.3 L'appétence pour le risque et la tolérance au risque 15
      4.1.4 L'analyse des risques 16
   4.2 Stratégies de traitement des risques 16

5. Évaluation des SI — une vue d'ensemble 18

6. Comprendre l'importance des contrôles des SI 22
   6.1 Les contrôles généraux et applicatifs des SI 22
      6.1.1 Les contrôles généraux 22
      6.1.2 Les contrôles applicatifs 23
   6.2 Les contrôles de la gouvernance, du management et techniques des SI 23
      6.2.1 Les contrôles de la gouvernance des SI 24
      6.2.2 Les contrôles du management 24
      6.2.3 Les contrôles techniques 24
      6.2.4 Les contrôles applicatifs 24
   6.3 Quels contrôles des SI ? 24
      6.3.1 Règles et procédures 25
      6.3.2 Normes 25
      6.3.3 Organisation et management 26
      6.3.4 Contrôles physiques et environnementaux 27
      6.3.5 Contrôles des logiciels systèmes 28
      6.3.6 Contrôles de l'acquisition et de développement des systèmes 28
      6.3.7 Contrôles applicatifs 29
   6.4 Sécurité informatique 30
   6.5 Cadre de contrôle des SI 30

7. Compétences et savoir-faire dans le domaine de l'audit des SI 31

8. Utilisation du cadre de contrôle 32
   8.1 Techniques d'audit assisté par ordinateur et analyse des données 32
   8.2 Recours à l'évaluation automatisée des risques 33
   8.3 Reporting des contrôles des SI 33

9. Conclusion 35

Auteurs et réviseurs 36

Annexe : Liste de vérification du Cadre de contrôles des SI 37

A propos du CRIPP 39

Résumé

Ce guide pratique d'audit des technologies (GTAG) aide les responsables de l'audit interne (RAI) et les auditeurs internes à rester en phase avec l'univers en constante évolution et parfois complexe des systèmes d'information (SI), en proposant un document destiné aux dirigeants d'entreprise - et non aux responsables des SI. La direction générale et le Conseil attendent de l'audit interne qu'il donne une assurance concernant les risques majeurs, notamment ceux introduits ou induits par la mise en œuvre des SI. La série des GTAG aide les RAI et les auditeurs internes à mieux comprendre les risques liés aux SI ainsi que les problématiques de contrôle et de gouvernance y afférents.

Ce GTAG a pour objectif d'aider les auditeurs internes à mieux appréhender les contrôles généraux des SI de façon à pouvoir échanger avec leur Conseil et partager des idées sur les risques et les contrôles avec le directeur des systèmes d'information. Ce GTAG décrit la façon dont la direction générale, le management, les spécialistes des systèmes d'information et les auditeurs internes gèrent les problématiques importantes relatives aux risques et aux contrôles, et présente des cadres pertinents pour évaluer les risques et les contrôles des SI. En outre, il pose les bases des GTAG suivants, qui sont consacrés à des sujets plus précis et présentent avec plus de détails les fonctions et responsabilités correspondantes dans l'entreprise.

Ce guide est la deuxième édition du premier volet de la série des GTAG - GTAG 1 : « Les contrôles des systèmes d'information » - publié en mars 2005.

1. Introduction

Ce GTAG a pour objectif d'expliquer les risques et les contrôles des SI afin de permettre aux RAI et aux auditeurs internes de comprendre et de communiquer sur la nécessité de disposer de solides contrôles des SI. Ce GTAG présente les composantes clés de l'évaluation des contrôles des SI, en mettant l'accent sur les fonctions et les responsabilités des principaux acteurs de l'organisation qui peuvent dicter la gouvernance des SI. Certains lecteurs reconnaîtront peut-être des éléments de ce GTAG, toutefois certaines parties offrent de nouvelles perspectives sur la façon d'aborder les risques et les contrôles des SI. L'un des objectifs de la série des GTAG est d'utiliser différentes composantes de l'évaluation des contrôles des SI comme moyens de sensibilisation aux risques et aux contrôles des SI ainsi qu'aux raisons pour lesquelles la direction générale et les auditeurs internes devraient veiller à ce qu'un environnement de contrôle efficace et pérenne soit mis en place pour maîtriser les risques liés aux SI.

Bien que la technologie offre des opportunités de croissance et de développement, elle s'accompagne également de menaces telles que des dysfonctionnements, des manœuvres répréhensibles, des vols et des fraudes. Les recherches montrent que les organisations sont menacées par des attaques externes, néanmoins les personnes de confiance, bien informées, représentent une menace bien plus importante. Heureusement, la technologie peut également protéger des menaces, comme le montre ce guide. Les dirigeants devraient être en mesure de poser les questions appropriées et d'appréhender les réponses apportées. Par exemple :

- Pourquoi devrais-je comprendre les risques et les contrôles des SI ? La réponse tient en deux mots : assurance et fiabilité. Les dirigeants jouent un rôle clé dans l'assurance de la fiabilité des informations. L'assurance repose sur un ensemble de contrôles métier interdépendants, ainsi que sur des preuves que les contrôles sont continus et suffisants. Le management doit examiner les preuves résultant de ces contrôles et des missions d'audit et conclure qu'ils donnent une assurance raisonnable.

- Que signifie être protégé ? La confiance représente le fondement de l'organisation et de son efficacité. Ainsi, la fiabilité des informations et des processus financiers – obligatoires pour de nombreuses organisations – repose sur la confiance. Cette confiance s'appuie sur des contrôles qui passent souvent inaperçus car ils sont intégrés dans le SI.

- Dans quels domaines les contrôles des SI s'appliquent-ils ? Dans tous les domaines. Les SI englobent les composantes, les processus, les ressources humaines, l'organisation et l'architecture technologiques, ainsi que les informations. Bon nombre de contrôles des SI sont de nature technique, et les SI fournissent les outils pour un grand nombre de contrôles métiers.

- Qui est responsable ? Chacun est responsable. Toutefois, l'affectation du contrôle et des responsabilités doit être définie et communiquée par le management, faute de quoi personne ne sera effectivement responsable, ce qui peut entraîner de graves conséquences.

- Quand les risques et les contrôles des SI devraient-ils être évalués ? Toujours. L'environnement des SI, qui favorise l'évolution des processus et de l'organisation, connaît des changements rapides. De nouveaux risques émergent rapidement. Les contrôles doivent apporter continuellement la preuve de leur efficacité, preuve qui doit être appréciée et évaluée constamment.

- Quel est le niveau de contrôle suffisant ? Il appartient au management d'en décider, en fonction l'appétence pour le risque, de la tolérance au risque et des réglementations en vigueur. Les contrôles ne représentent pas un objectif ; ils visent à contribuer à la réalisation des objectifs de l'organisation. Les contrôles constituent un coût intrinsèque à l'activité, qui

peut être élevé, mais sans commune mesure avec les éventuelles conséquences de contrôles inadéquats.

Les contrôles des SI sont essentiels pour protéger les actifs, les clients, les partenaires et les données sensibles, pour faire preuve d'un comportement sûr, efficace et éthique, et pour préserver la marque, la réputation et la confiance. Dans l'environnement actuel de mondialisation et de réglementation, il est facile de perdre ces actifs. Un RAI peut s'appuyer sur ce guide pour évaluer le cadre et les pratiques d'audit interne de l'organisation dans le domaine des risques et des contrôles des SI, de la conformité et de l'assurance. Ce guide peut également être utilisé pour relever les défis inhérents à des menaces qui changent constamment, sont de plus en plus complexes et évoluent rapidement, ainsi qu'à la nécessité d'accroître l'efficacité.

Les contrôles des SI n'existent pas isolément. Ils forment un dispositif continu de protection dont les éléments sont interdépendants, et dont l'intégrité peut être compromise si les liens entre eux sont peu solides. Potentiellement sujets à des erreurs et des contournements, les contrôles des SI vont du plus simple au plus complexe, et s'intègrent dans un environnement dynamique. Les contrôles des SI comportent principalement deux volets : l'automatisation des contrôles métiers (en appui du management de l'organisation et de la gouvernance) et le contrôle de l'environnement des SI et des activités (en appui des applications et de l'infrastructure des SI). Le RAI doit prendre en compte et évaluer ces deux éléments. Il peut considérer les contrôles métiers automatisés comme étant les contrôles nécessitant le regroupement de compétences d'audit opérationnel et d'audit informatique associées sous la forme d'audit intégré. Le RAI peut également souhaiter séparer les contrôles généraux des SI ou les contrôles informatiques généraux sur la base des compétences techniques nécessaires pour évaluer des applications, infrastructures et activités plus techniques. Ainsi, un Progiciel de Gestion Intégré (PGI aussi appelé ERP - enterprise resource planning) fait davantage appel à des connaissances techniques et opérationnelles pour comprendre et évaluer les contrôles des structures de la base de données, des accès utilisateurs, de la configuration du système et du reporting financier. Le RAI constatera que l'évaluation des infrastructures telles que les réseaux, les routeurs, les pare-feux et les appareils sans fil et mobiles exige des compétences et une expérience spécifiques. Pour les contrôles des SI, l'auditeur interne doit tout d'abord disposer d'une bonne compréhension des concepts avant de pouvoir tirer les conclusions d'une évaluation des risques et des contrôles. L'audit interne suppose une interaction forte avec les personnes ayant des responsabilités de contrôles, et requiert un maintien à jour des connaissances, et des évaluations continues en fonction de l'émergence de nouvelles technologies, et de l'évolution des opportunités, usages, dépendances, stratégies, risques et besoins de l'organisation.

Les contrôles des SI apportent une assurance quant à la fiabilité de l'information et des services rendus. Ils permettent d'atténuer les risques inhérents à l'usage des SI. Il peut s'agir des politiques de l'organisation aussi bien que de leur mise en œuvre dans des programmes informatiques, de la protection des accès physiques à la capacité de tracer les actions et les transactions des utilisateurs, de validations automatiques ou encore des analyses de cohérence pour de grands volumes de données.

Les exemples suivants illustrent des concepts essentiels de ces contrôles :

- Les contrôles des SI présents dans le système de contrôle interne fournissent une assurance quant au niveau de maîtrise des risques. Ces contrôles doivent être continus et s'appuyer sur des éléments de preuve traçables et fiables.
- L'assurance de l'auditeur interne est une évaluation indépendante et objective du bon fonctionnement des contrôles des SI. Cette assurance repose sur la compréhension, l'examen et l'évaluation des contrôles clés liés aux risques qu'ils doivent traiter, et sur la réalisa-

tion de tests suffisants pour s'assurer de la conception adéquate des contrôles et de leur fonctionnement efficace et continu.

De nombreux cadres de référence permettent de catégoriser les contrôles des SI et leurs objectifs. Ce guide recommande que chaque organisation emploie les composantes applicables des cadres de référence existants pour catégoriser et évaluer les risques et les contrôles des SI.

2. Fondamentaux concernant les risques et les contrôles des SI

2.1 Concepts clés

Les organisations continuent d'exploiter l'évolution constante de la technologie pour développer leur offre et leurs services, nécessitant ainsi une adaptation de la profession d'audit interne. Les *Normes internationales pour la pratique professionnelle de l'audit interne* de l'IIA (les Normes) précisent que les auditeurs internes doivent évaluer les risques et les contrôles pour les systèmes d'information de l'organisation. Avec les GTAG, l'IIA donne une autre perspective sur l'évaluation des risques et des contrôles des SI. Le GTAG 4 « Management de l'audit des systèmes d'information » aborde l'analyse les risques liés aux SI et l'univers des risques des SI qui en découle. Le GTAG 11 « Élaboration d'un plan d'audit des SI » aide l'audit interne à évaluer les processus métiers soutenus par la technologie et les éventuels composants de l'univers d'audit des SI. En outre, le GTAG 8 « Audit des contrôles applicatifs » couvre les aspects propres à l'audit des contrôles applicatifs et l'approche pouvant être adoptée par l'audit interne lors de l'évaluation de ces contrôles.

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

Comme plus amplement analysé dans ce GTAG, l'évaluation des risques et des contrôles des SI mis en place pour les gérer doit être associée à l'environnement des processus métiers et aux objectifs spécifiques de l'organisation devant être atteints, conformément aux attentes des dirigeants et du Conseil. Les risques liés aux SI, qui ne représentent qu'une partie de l'interconnexion complexe des personnes, des processus, de l'infrastructure et de l'environnement de risque existant, devraient être gérés de façon globale par l'organisation.

Les auditeurs internes doivent comprendre l'éventail des contrôles dont ils disposent pour limiter les risques liés aux SI. Les contrôles peuvent être envisagés selon une séquence qui tient compte de leur interconnexion et du fait que l'échec d'un ensemble de contrôles peut entraîner une dépendance accrue et la nécessité d'un examen des autres groupes de contrôle. Les contrôles SI traités dans ce document sont de différents ordres selon la personne qui les met en œuvre et les gère au sein de l'organisation. Il peut s'agir de contrôles au niveau de la gouvernance, du management ; de contrôles techniques ou applicatifs (cf. §6.2).

On peut aussi considérer les contrôles des SI sous l'angle des contrôles généraux des SI et des contrôles applicatifs. Les contrôles généraux des SI sont, par nature, fondamentaux et sont revus au travers de différentes méthodes d'audit. Citons par exemple l'exploitation des SI, le développement et la maintenance d'applications, la gestion des utilisateurs, la gestion des changements, ainsi que la sauvegarde et la restauration de données. Les contrôles applicatifs représentent une autre catégorie de contrôles et englobent les contrôles des données en entrée, des traitements, et des données en sortie.

Ce GTAG analyse également l'utilisation des contrôles dans le cadre de la gestion et du pilotage de l'infrastructure, des processus et du personnel soutenant l'organisation au travers de la technologie. La gouvernance des SI continue d'évoluer au sein des organisations en raison de l'utilisation continue des SI, et de la supervision accrue par la direction générale et le Conseil.

2.2 Gouvernance des SI

Un aspect important de la question des contrôles des SI est celle de la gouvernance des SI, qui offre un cadre garantissant que les SI peuvent répondre aux besoins opérationnels de l'organisation. Pour le management des SI, il est important d'acquérir une solide compréhension des processus métiers de l'organisation utilisés pour atteindre ses objectifs et atteindre les buts fixés par la direction générale et le Conseil. La gouvernance des SI ne se limite pas aux contrôles nécessaires à la gestion des risques identifiés, mais représente également une structure intégrant des pratiques et le personnel informatique. Elle doit être étroitement alignée sur les stratégies et objectifs de l'organisation, pour en permettre leur réalisation.

Un RAI doit pouvoir évaluer la structure de gouvernance des SI et sa capacité à produire des résultats pour l'organisation, et accroître l'efficience des activités informatiques. Les recherches montrent que la gouvernance des SI se traduit par une amélioration de la performance opérationnelle, et par un meilleur alignement des SI avec l'entreprise dans la réalisation de ses objectifs stratégiques.

La gouvernance des SI englobe le leadership, les structures organisationnelles et les processus assurant que les SI de l'organisation maintiennent et soutiennent les stratégies et objectifs de l'organisation.

La Norme 2110.A2 de l'IIA précise que l'audit interne doit évaluer si la gouvernance des SI de l'organisation soutient la stratégie et les objectifs de l'organisation ; les RAI doivent donc être prêts à évaluer cet aspect clé de l'environnement global des SI.

Une bonne application des principes de gouvernance des SI peut influencer et affecter l'ensemble de l'organisation et son interaction avec les SI.

- **Identifier et gérer les risques liés aux SI et permettre une amélioration des SI :** la gouvernance des SI contribue à assurer l'existence d'un lien étroit avec les activités de gestion des risques d'une organisation, notamment le management des risques de l'entreprise (ERM). La gouvernance des SI doit faire partie intégrante de la gestion globale des risques de l'organisation, de sorte que les techniques appropriées puissent être intégrées aux activités des SI, notamment la communication sur l'état des risques (aux principales parties prenantes) dans l'ensemble de l'organisation. Le RAI devrait revoir les activités de gestion des risques mises en œuvre dans l'ensemble de l'organisation et veiller à ce qu'il existe des liens entre efforts de gestion des risques des SI et activités risquées de l'organisation, et à ce que le profil de risque des SI reçoive l'attention appropriée.

- **Renforcer la relation entre les directions métiers et la direction des SI :** la gouvernance des SI établit un mécanisme reliant l'utilisation des SI aux stratégies et objectifs de l'organisation. La relation entre les directions métiers et la direction des SI (DSI) permettra de veiller à ce que les ressources informatiques fassent ce qu'il faut au moment opportun. La communication entre la DSI et les directions métiers devrait être fluide et informative, donnant des éclairages sur les apports des SI, ainsi que sur l'état d'avancement de ses efforts. Le RAI devrait revoir cet alignement, et s'assurer de l'existence de solides processus de gestion du portefeuille applicatif qui permettent aux directions métiers et à la DSI de collaborer sur les initiatives et sur les décisions d'investissement globales.

- **Obtenir une visibilité sur la capacité du management des SI à réaliser ses objectifs :** la DSI définira sa stratégie en appui de l'organisation, ce qui consiste pour partie à veiller à l'exploitation efficiente et sans compromis des SI au quotidien. Les indicateurs et les objectifs sont définis non seulement pour aider la DSI à délivrer et opérer les SI, mais également pour guider les activités des informaticiens vers une amélioration de la maturité de ses pratiques.

Les résultats permettront à la DSI d'exécuter sa stratégie et d'atteindre les objectifs approuvés par le management de l'organisation. Le RAI devrait évaluer si le lien entre indicateurs et objectifs des SI est aligné sur ceux de l'organisation et mesure la progression des initiatives approuvées. En outre, le RAI peut aider à valider que les indicateurs sont correctement mesurés et qu'ils donnent une image réaliste de l'exploitation et de la gouvernance des SI sur les plans tactique et stratégique.

- **Gérer les risques et identifier les opportunités d'amélioration continue pour l'organisation et les conséquences pour les SI :** la gestion des risques est une composante clé d'une structure de gouvernance des SI efficace au sein d'une organisation. L'identification et la gestion des risques liés aux SI permettront à la DSI de fonctionner plus efficacement, tout en identifiant des opportunités potentielles d'amélioration de ses pratiques. Les risques liés aux SI devraient être rattachés à des propriétaires, qui communiquent méthodiquement sur l'état d'avancement des efforts de gestion des risques à tous les niveaux de l'organisation. Le RAI joue un rôle important lorsqu'il valide la cohérence de l'univers des risques liés aux SI. Il utilisera les informations pour aider à définir l'univers de l'audit interne en vue d'une évaluation des risques indépendante et de l'élaboration du plan d'audit. Le *Risk IT Practitioner Guide* élaboré par l'IT Governance Institute (ITGI) et l'ISACA offre un cadre de référence pour l'identification et l'évaluation des risques liés aux SI, tout en établissant un lien direct avec le cadre de référence COBIT *(Control Objectives for Information and Related Technology).*

- **Améliorer, grâce à la gouvernance des SI, la flexibilité des SI en réponse aux évolutions de l'organisation et de l'environnement des SI :** la gouvernance des SI offre des bases permettant à la DSI de mieux gérer ses responsabilités et d'apporter un meilleur soutien à l'organisation grâce à des processus ainsi que des rôles et responsabilités de son personnel informatique clairement définis. Ce type de formalisation permet aux SI de mieux identifier les anomalies potentielles au quotidien et leur évolution tendancielle, et donc d'identifier la cause à l'origine des constats et des dysfonctionnements. En outre, la DSI a la capacité de s'adapter plus facilement aux demandes ponctuelles de capacités opérationnelles nouvelles ou accrues. Aujourd'hui, le RAI peut utiliser ces sources de données (par exemple le support technique et les tickets de gestion de problèmes) pour évaluer comment les SI gèrent les problèmes inconnus. Le RAI peut également examiner les processus de gestion de portefeuille des SI pour comprendre la façon dont les besoins sont hiérarchisés, et s'il existe une flexibilité pour définir une nouvelle priorité des besoins en fonction des évolutions des priorités de l'organisation.

Lorsqu'il évalue la structure et les pratiques de gouvernance des SI d'une organisation, l'audit interne peut examiner plusieurs composantes clés qui conduisent à une gouvernance efficace des SI, notamment :

- **Le leadership.** Évaluer la relation entre les objectifs des SI et les besoins actuels et stratégiques de l'organisation. Évaluer l'implication des responsables informatiques dans le développement et la concrétisation des objectifs stratégiques de l'organisation. Examiner les modalités d'affectation des rôles et des responsabilités au sein de l'activité des SI, et si le personnel les exécute comme prévu. Examiner également la contribution de la direction générale et du Conseil pour instaurer et maintenir une solide gouvernance des SI.

- **Les structures organisationnelles.** Examiner comment le personnel informatique et les directions métiers interagissent et communique les besoins actuels et futurs dans le cadre de la structure organisationnelle existante. Cet exercice devrait couvrir l'existence des fonctions nécessaires et des rattachements hiérar-

chiques permettant à la DSI de répondre convenablement aux besoins opérationnels tout en permettant aux demandes du métier d'être gérées via une évaluation et une hiérarchisation formelles.

- **Les processus des SI.** Évaluer les activités et les contrôles des SI existants pour gérer les besoins opérationnels, tout en donnant l'assurance nécessaire sur les processus métiers et les systèmes sous-jacents. L'activité des SI utilise les processus pour soutenir l'environnement des SI et contribuer à l'homogénéité des services fournis. Déterminer comment la DSI sera évaluée sur sa faculté à aider l'organisation à atteindre ses objectifs.

- **La gestion des risques.** Examiner les processus de l'activité des SI pour identifier, évaluer et suivre / atténuer les risques dans l'environnement des SI. En outre, identifier les responsabilités confiées au personnel au sein du processus de gestion des risques, et déterminer s'il s'acquitte de ces responsabilités conformément aux attentes. Comprendre les événements qui se sont produits et ont affecté l'activité des SI pour déterminer si des pratiques de gestion des risques appropriées sont mises en œuvre, et si les données sur les risques (par exemple leur fréquence, leur impact, les techniques d'atténuation) sont convenablement documentées et, le cas échéant, mises à jour après l'événement.

- **Les activités de contrôle.** Évaluer les principaux contrôles définis par la DSI pour gérer l'activité et soutenir l'ensemble de l'organisation. L'audit interne devrait revoir les aspects liés à la propriété, la documentation et l'autovalidation. En outre, l'ensemble des contrôles devrait être suffisamment solide pour maîtriser les risques identifiés.

3. Parties prenantes internes et responsabilités des SI

Une organisation doit comprendre et gérer son environnement des SI. Elle doit en outre comprendre et reconnaître la dépendance des processus métiers envers les SI et la nécessité de respecter les exigences réglementaires.
Une bonne ou une mauvaise gestion ou utilisation des SI peut permettre de tirer parti ou de manquer des opportunités commerciales. Une gouvernance efficace des SI accroît la probabilité que les SI facilitent la réalisation des objectifs de l'organisation, et que les ressources soient gérées avec prudence. Le tableau ci-après[1] expose un ensemble de responsabilités de surveillance pouvant être exercées par le Conseil, la direction générale, la DSI et les auditeurs internes du point de vue de la gouvernance des SI.

Rôle	Responsabilité
Le Conseil	**Le Conseil devrait :** • Comprendre la valeur stratégique de la fonction informatique. • S'informer du rôle et de l'impact des SI sur l'organisation. • Fixer une direction stratégique et anticiper un retour. • Examiner la façon dont le management attribue les responsabilités. • Superviser la transformation. • Comprendre les contraintes dans lesquelles opère la direction générale. • Superviser l'alignement de l'organisation par rapport à la stratégie. • Demander à la direction générale de dégager une valeur mesurable au travers des SI. • Superviser les risques de l'organisation. • Favoriser l'apprentissage, le développement et la gestion des ressources. • Superviser l'évaluation des performances. • Obtenir une assurance.
La direction générale	**La direction générale devrait :** • S'informer du rôle et de l'impact des SI sur l'organisation. • Diffuser la stratégie, les politiques et les objectifs à tous les niveaux de l'organisation et aligner la structure des SI avec les objectifs de l'organisation. • Déterminer les capacités et les investissements nécessaires. • Affecter les responsabilités. • Soutenir les activités en cours. • Fournir les structures et les ressources organisationnelles nécessaires. • Intégrer des responsabilités claires pour la gestion des risques et le contrôle des SI. • Évaluer la performance. • Privilégier les compétences stratégiques que les SI doivent soutenir. • Privilégier les processus majeurs des SI qui créent de la valeur. • Créer une organisation flexible et adaptable qui exploite informations et connaissances. • Renforcer la valeur de l'offre de services. • Élaborer des stratégies pour optimiser les coûts des SI. • Disposer de stratégies d'acquisition des compétences claires.

[1] *Le tableau contient des parties du Board Briefing on IT Governance de l'ITGI, 2e édition, utilisées avec l'aimable autorisation de l'ITGI et l'ISACA. ©2003 ITGI. Tous droits réservés.*

La DSI	**La DSI devrait :** • Gérer les attentes de la direction générale en matière de SI. • Piloter le développement de la stratégie des SI et sa mise en œuvre. • Relier les budgets des SI aux buts et objectifs stratégiques. • S'assurer qu'une valeur mesurable est dégagée dans les délais et le budget impartis. • Établir des normes, des politiques et un cadre de contrôle des SI, selon les besoins. • Informer et former le management sur les problématiques des SI. • Rechercher des manières d'accroître la contribution des SI à la création de valeur. • Veiller à la bonne gestion des projets informatiques. • Fournir des infrastructures informatiques qui facilitent une création et un partage rentables de l'informatique décisionnelle. • Veiller à la disponibilité de ressources, de compétences et d'infrastructures des SI nécessaires à la réalisation des objectifs et à la création de valeur. • Évaluer les risques, les atténuer efficacement, et les rendre transparents pour les parties prenantes. • S'assurer que les rôles essentiels à la gestion des risques des SI sont convenablement définis et dotés en ressources. • Veiller à la gestion et à la vérification au quotidien des processus et des contrôles des SI. • Mettre en place des indicateurs de performance liés directement et manifestement à la stratégie. • Privilégier les compétences clés dans le domaine informatique.
L'audit interne	**L'audit interne devrait :** • Veiller à posséder un niveau minimal d'expertise en SI suffisant. • Inclure l'évaluation des SI dans son processus de planification. • Évaluer si la gouvernance des SI dans l'organisation soutient et conforte les stratégies et les objectifs. • Identifier et évaluer les expositions de l'organisation aux risques liés aux SI. • Évaluer les contrôles mis en place en réponse aux risques au sein des SI de l'organisation. • Veiller à posséder l'expertise nécessaire en matière de SI pour s'acquitter de ses responsabilités. • Envisager, le cas échéant, d'utiliser des techniques d'audit informatisées.

Outre les parties prenantes internes, les parties extérieures telles que les auditeurs externes, les autorités nationales, les attentes du public et les organisations internationales de normalisation doivent être prises en compte.

4. L'analyse des risques

Les contrôles des SI sont choisis et mis en œuvre en fonction des risques qu'ils sont censés traiter. Une fois les risques identifiés, la stratégie de traitement des risques à adopter peut aller de : ne rien faire et accepter le risque comme un coût intrinsèque à l'activité, ou appliquer divers contrôles spécifiques, notamment souscrire une police d'assurance.

Il serait relativement simple d'établir une liste de contrôles des SI à mettre en œuvre impérativement dans chaque organisation. Cependant, chaque contrôle induit un coût spécifique qui peut ne pas se justifier du point de vue de la rentabilité, suivant le type d'activités réalisées par l'organisation. En outre, aucune liste de contrôles n'est applicable à toutes les catégories d'organisations. Même si l'on peut formuler de multiples conseils sur le choix des contrôles adéquats, il faut faire preuve de discernement et de jugement. Les contrôles doivent être adaptés au niveau de risque auquel doit faire face l'organisation. Le RAI doit pouvoir conseiller le comité d'audit sur la fiabilité du cadre de contrôle interne et fournir un niveau d'assurance approprié selon l'appétence pour le risque affiché par l'organisation. Le COSO[1] définit l'appétence, pour le risque de l'organisation comme :
« Le niveau de risque global qu'une organisation accepte de prendre pour répondre à son objectif de création de valeur. […] L'appétence pour le risque est prise en compte dans la définition de la stratégie dans la mesure où les résultats de la stratégie doivent être en ligne avec l'appétence pour le risque. [...] La direction tient compte de l'appétence pour le risque lorsqu'elle […] élabore son dispositif pour traiter les risques et les gérer efficacement. »
En plus de l'appétence au risque, le responsable de l'audit interne doit prendre en considération la tolérance au risque, que le COSO définit comme :
« Le niveau de variation que l'entité accepte quant à l'atteinte d'un objectif spécifique. […] Lorsqu'elle définit le seuil de tolérance au risque, la direction considère l'importance relative des objectifs et aligne la tolérance au risque avec l'appétence pour le risque. »
Ainsi, le responsable de l'audit interne doit évaluer si oui ou non :

- L'environnement informatique de l'organisation est cohérent avec l'appétence pour le risque de l'organisation.
- Le cadre de contrôle interne est adéquat pour que les opérations de l'organisation restent dans les limites des tolérances au risque énoncées.

4.1 Prise en compte du risque dans l'évaluation de l'adéquation des contrôles des SI

La gestion du risque s'applique à l'ensemble des activités de l'organisation, et pas seulement à l'utilisation des SI. On ne peut pas considérer les SI isolément : ils font partie intégrante de tous les processus. Le choix des contrôles des SI ne se résume pas à appliquer les bonnes pratiques recommandées. Ces contrôles doivent apporter une valeur ajoutée à l'organisation en réduisant efficacement les risques et en améliorant l'efficacité.

Lorsque le RAI cherche à savoir si les contrôles des SI sont adéquats au sein du cadre de contrôle interne de l'organisation, il doit étudier les processus établis par la direction générale afin de déterminer :

- L'utilisation, la valeur et le caractère critique des données.
- L'appétence pour le risque et la tolérance au risque de l'organisation pour chaque fonction et processus.
- Les risques informatiques auxquels est confrontée l'organisation, et la qualité du service offert à ses utilisateurs.
- La complexité de l'infrastructure SI.
- Le caractère adéquat des contrôles des SI et leur utilité.

[1] *The Committee of Sponsoring Organizations of the Treadway Commission,"Committee of Sponsoring Organizations for the Commission on Fraudulent Financial Reporting."www.coso.org.*

La fréquence de l'analyse de risques est un élément important, fortement influencé par les changements internes et externes. La rapidité des évolutions technologiques impactera chaque organisation différemment. Certaines organisations auront besoin de répondre très rapidement aux risques associés à ces évolutions alors que d'autres décideront d'être plus attentistes.

4.1.1 L'environnement des SI

L'analyse et l'évaluation des risques informatiques peuvent se révéler complexes. L'infrastructure SI se compose de matériels, de logiciels, de communications, d'applications, de protocoles (règles) et de données. Ces composantes doivent être déployées dans un espace physique, au sein de l'organisation et entre l'organisation et son environnement externe. L'infrastructure inclut également les personnes qui interagissent avec les éléments physiques et logiques des systèmes.

Les autres zones de risque à prendre en considération incluent celles qui sont associées aux projets ainsi qu'aux relations avec les fournisseurs. Un des risques associés aux projets est par exemple, la sous-évaluation du budget, des ressources, des compétences techniques. Pour les risques liés aux relations avec les prestataires de service ou les fournisseurs, l'auditeur informatique devra notamment se poser la question de la pérennité, de la solvabilité du prestataire, de la revue des contrôles informatiques et des clauses d'audit.

L'inventaire des composantes de l'infrastructure SI met en lumière des informations de base sur les vulnérabilités de l'environnement. Ainsi, les systèmes et réseaux connectés à Internet sont exposés à des menaces que ne connaissent pas les systèmes et réseaux autonomes. Parce que la connectivité à Internet est essentielle pour la plupart des systèmes et réseaux, les organisations doivent veiller à ce que ceux-ci intègrent les contrôles fondamentaux qui assurent une sécurité de base.

L'évaluation des vulnérabilités au sein des infrastructures informatiques commence par un inventaire complet du matériel, des logiciels, réseaux et données de l'organisation. Les schémas d'architecture des systèmes font apparaître l'agencement des composants de l'infrastructure et la manière dont ils interagissent avec d'autres composants, à l'intérieur et en dehors de l'organisation. Pour les experts en sécurité informatique, l'inventaire et l'architecture des composants (y compris le positionnement des technologies et contrôles de sécurité) permettent de révéler les éventuelles vulnérabilités. Malheureusement, les informations concernant un système ou un réseau peuvent aussi rendre les vulnérabilités apparentes aux yeux d'un pirate potentiel, si bien que l'accès à ces informations doit être limité aux seules personnes qui en ont besoin. Un environnement de systèmes et de réseau correctement configuré permet de minimiser la quantité d'informations mises à disposition des éventuels pirates, et un environnement qui paraît sécurisé représente une cible bien moins attrayante pour la plupart des pirates.

4.1.2 Les risques informatiques rencontrés par l'organisation

Le RAI s'entretient des risques informatiques avec le directeur des SI et les propriétaires des processus afin de s'assurer que toutes les parties concernées ont une compréhension et une conscience suffisantes des risques techniques auxquels doit faire face l'organisation du fait de son utilisation des SI, et du rôle qui est le leur dans la mise en place et la maintenance de contrôles efficaces.

4.1.3 L'appétence pour le risque et la tolérance au risque

Fort de sa connaissance des risques informatiques, l'auditeur peut valider l'existence de contrôles efficaces, correspondant à l'appétence pour le risque défini par l'organisation et sa tolérance aux risques informatiques. Pour procéder à cette évaluation, l'auditeur devra discuter avec de nombreux managers et dirigeants, et éventuellement avec le Conseil. Le niveau de détails de ces discussions sera déterminé en sollicitant l'avis du directeur des SI, du RSSI, et des propriétaires de processus.

Les organisations qui mettent en œuvre l'ERM, devront prendre en considération les risques des SI. L'ERM comprend des méthodes et des processus pour gérer les risques et saisir toutes les opportunités pour réaliser les objectifs de l'organisation. Il faut généralement commencer par l'identification d'événements ou de circonstances pertinents par rapport aux objectifs de l'organisation (par exemple, les risques de fuite d'information), puis les évaluer en termes de probabilité et d'impact (par exemple, le risque inhérent d'une fuite d'information est fort, et l'impact est également élevé), pour déterminer une réponse (par exemple, de nouvelles règles pour mieux sécuriser les données de l'organisation) et suivre les progrès accomplis dans la mise en œuvre de réponses (par exemple, la mise en place de nouvelles mesures de sécurité dans les SI pour éviter des fuites d'information). En identifiant et en anticipant les risques et les opportunités, les organisations seront plus à même de se protéger et de créer de la valeur pour les parties prenantes. Ainsi, l'ERM aide le responsable de l'audit interne dans la compréhension des risques majeurs de l'organisation. Ensuite, le RAI peut l'utiliser pour fixer les priorités de l'audit interne, déterminer les missions d'audit et la tolérance et l'appétence au risque.

4.1.4 L'analyse des risques

Une analyse des risques doit impliquer différentes fonctions et directions telles que le responsable de la gestion des risques, le RAI, la direction des SI et des responsables métiers.

Les questions fondamentales de l'évaluation des risques sont :

- Quels actifs informatiques (actifs tangibles ou intangibles, comme l'information ou la réputation) sont exposés à un risque ? Quel est le niveau de confidentialité, d'intégrité et de disponibilité nécessaire pour chacun de ces actifs ?
- Quel événement (menace) pourrait influer négativement la valeur de ces actifs informationnels ? Cette question sous-entend l'analyse de la vulnérabilité et la cartographie des vulnérabilités face aux menaces ainsi que les données susceptibles d'être affectées.
- Si une menace venait à se réaliser, quelle serait la gravité de ses répercussions ?
- À quelle fréquence peut-on s'attendre à voir ces événements se réaliser ?
- Quel est le degré de certitude des réponses aux quatre premières questions (analyse d'incertitude) ?
- Que peut-on faire pour réduire le risque ?
- Quel en sera le coût ?
- Est-ce rentable ?

Déterminer la valeur des données traitées et stockées n'est pas chose facile, en raison des multiples dimensions de cette valeur. Le RAI pourra tirer parti d'une coordination avec le responsable de la gestion des risques et s'aligner sur les risques liés au SI. En fonction de la taille de l'organisation et de ses risques, le RAI et le responsable de la gestion des risques peuvent partager leurs méthodes de hiérarchisation des risques, de couverture des risques et utiliser leurs ressources de manière plus efficiente.

4.2 Stratégies de traitement des risques

Une fois les risques identifiés et analysés, il n'est pas toujours judicieux de mettre en œuvre des mesures visant à les contrer. Certains risques peuvent avoir un impact mineur ou être extrêmement peu probables, et il peut s'avérer peu rentable d'adopter des procédures de contrôle onéreuses pour y remédier.

De manière générale, il existe plusieurs manières de traiter les risques :

- **Accepter le risque.** L'une des principales fonctions du management consiste à gérer le risque. Certains risques sont mineurs parce que leurs répercussions et leur probabilité sont faibles. Dans ce cas, on recommande d'accepter sciemment le risque comme constituant un coût inhérent à l'activité, et de réévaluer périodiquement ce risque pour s'assurer que ses répercussions restent faibles.

- **Eviter le risque.** Il est possible qu'un risque découle du recours à une technologie, à un fournisseur ou à un éditeur en particulier. On peut alors l'éviter en remplaçant ladite technologie par des produits plus robustes, ou en recherchant des fournisseurs ou des distributeurs plus performants.
- **Partager le risque.** L'atténuation du risque peut être partagée avec les partenaires commerciaux et les fournisseurs. Un bon exemple réside dans l'externalisation de la gestion de l'infrastructure. Dans ce cas, les risques découlant de la gestion de l'infrastructure SI sont atténués par le fournisseur qui dispose de capacités accrues et a accès à du personnel mieux qualifié que son client. Le risque peut également être réduit par le transfert des coûts de la réalisation du risque à une compagnie d'assurance.
- **Réduire le risque.** En lieu et place ou en association avec d'autres options, il convient de concevoir des contrôles idoines et de les mettre en œuvre pour empêcher que le risque ne se réalise, pour réduire la probabilité d'occurrence ou en minimiser les effets.

5. Évaluation des SI – une vue d'ensemble

Les contrôles des SI mis en œuvre lors du contrôle ou de la maîtrise des risques se révèlent être la meilleure option. S'il convient d'appliquer les contrôles des SI en tenant dûment compte des risques concernés ; il existe un ensemble de contrôles élémentaires qui devraient être mis en place pour assurer un niveau minimum de contrôle des SI.

Les contrôles des SI devraient faire partie des principaux processus SI relatifs à la planification, l'organisation, les acquisitions, les changements, la prestation de services des SI, ainsi que le support et la surveillance des SI. Les contrôles des SI qui viennent en appui d'une large part de ces processus SI sont généralement des contrôles de l'infrastructure des SI couvrant des domaines tels que les contrôles réseau, les contrôles des bases de données, des systèmes opérationnels et du matériel. Les contrôles des SI couvrant des applications et, souvent, d'importants domaines opérationnels, peuvent inclure des contrôles de validation des saisies, des contrôles de réalisation de processus ou de rapprochements, et des contrôles des rapports d'anomalies. Pour comprendre les risques et les contrôles des SI, le RAI devrait en premier lieu acquérir une vue d'ensemble des contrôles importants et des processus métiers qu'ils soutiennent. Les descriptions des processus et les organigrammes comptent parmi les outils utiles pour acquérir une vue d'ensemble. En outre, le RAI devrait comprendre les principales initiatives technologiques pour appréhender l'évolution éventuelle des infrastructures et des applications des SI sur un intervalle de temps donné. Grâce à ces informations, le RAI pourra effectuer une évaluation initiale des risques qui permettra une analyse plus approfondie.

Certaines questions peuvent être prises en compte lors de l'évaluation de l'environnement de contrôle et de la sélection d'un ensemble approprié de contrôles.

- Existe-t-il une politique des SI, et notamment des contrôles des SI ?
- Les responsabilités en matière de SI et de contrôles des SI ont-elles été définies, affectées et acceptées ?
- La conception du contrôle est-elle efficace ?
- Le fonctionnement du contrôle est-il efficace ?
- Le contrôle aboutit-il au résultat souhaité ?
- La combinaison de contrôles préventifs, détectifs et correctifs est-elle efficace ?
- Les contrôles génèrent-ils des éléments de preuve lorsque les limites sont franchies ou que les contrôles échouent ? Comment le management est-il averti des dysfonctionnements, et quelles mesures sont attendues en conséquence ?
- Des traces sont-elles conservées (par exemple au travers d'une piste d'audit) ?
- Les équipements et outils d'infrastructure des SI bénéficient-ils d'une protection logique et physique ?
- Des mécanismes de contrôle d'accès et d'authentification sont-ils utilisés ?
- Existe-t-il des contrôles protégeant l'environnement opérationnel et les données des virus et autres logiciels malveillants ?
- Existe-t-il des contrôles relatifs aux pare-feux ?
- Existe-t-il des politiques relatives aux pare-feux ?
- Des évaluations des vulnérabilités externes et internes sont-elles effectuées et les risques ont-ils été identifiés et résolus de manière satisfaisante ?
- Existe-t-il des procédures d'assurance-qualité et de gestion des changements et de la configuration ?
- Existe-t-il des procédures structurées de surveillance et de mesures des services ?
- Les risques inhérents aux services externalisés ont-ils été pris en compte ? (Pour de plus amples informations sur ce point, voir le GTAG 7 : L'infogérance.)

Le secteur des cartes de paiement (PCI) publie des normes de sécurité des données parmi les plus couramment utilisées - PCI Data Security Standards (PCI DSS). Lancé en 2006, le Conseil des

normes de sécurité PCI est un forum international ouvert, en charge du développement, de la gestion, de l'éducation et de la sensibilisation aux normes de sécurité PCI, dont : la norme de sécurité des données (DSS), la norme de sécurité des données d'application de paiement (PA-DSS), et les besoins liés au service de saisie du PIN (PED).

Le RAI peut s'appuyer de façon importante sur la norme PCI DSS pour déterminer si certaines activités liées à la sécurité devraient être prises en compte pour l'organisation (voir la norme PCI DSS – Présentation).

Introduction et présentation de la norme PCI DSS

La norme PCI (Payment Card Industry) DSS (Data Security Standard) a été développée dans le but de renforcer la sécurité des données des titulaires de cartes et de faciliter l'adoption de mesures de sécurité uniformes à l'échelle mondiale. La norme PCI DSS sert de référence aux conditions techniques et opérationnelles conçues pour protéger les données des titulaires de cartes. La norme PCI DSS s'applique à toutes les entités impliquées dans le traitement des cartes de paiement, notamment les commerçants, les entreprises de traitement, acheteurs, émetteurs et prestataires de service, ainsi que toutes les autres entités qui stockent, traitent ou transmettent des données de titulaires de cartes. La norme PCI DSS consiste en un ensemble de conditions minimales pour la protection des données de titulaires de cartes et peut être renforcée par des contrôles et des pratiques supplémentaires afin de réduire davantage les risques. Les 12 conditions de la norme PCI DSS sont résumées ci-dessous.

PCI DSS – Présentation synthétique	
Création et gestion d'un réseau sécurisé	1. Installer et gérer une configuration de pare-feu pour protéger les données des titulaires de cartes. 2. Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut, définis par le fournisseur.
Protection des données des titulaires de cartes de crédit	3. Protéger les données de titulaires de cartes stockées. 4. Crypter la transmission des données des titulaires de cartes sur les réseaux publics ouverts.
Gestion d'un programme de gestion des vulnérabilités	5. Utiliser des logiciels antivirus et les mettre à jour régulièrement. 6. Développer et gérer des systèmes et des applications sécurisés.
Mise en œuvre de mesures de contrôle d'accès strictes	7. Restreindre l'accès aux données des titulaires de cartes aux seuls individus qui doivent les connaître. 8. Affecter un identifiant unique à chaque utilisateur d'ordinateur. 9. Restreindre l'accès physique aux données des titulaires de cartes.
Surveillance et tests réguliers des réseaux	10. Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données des titulaires de cartes. 11. Tester régulièrement les processus et les systèmes de sécurité.
Gestion d'une politique de sécurité des informations	12. Gérer une politique de sécurité des informations pour l'ensemble du personnel.

L'évaluation des contrôles des SI est un processus continu. Les procédures métiers changent constamment au fil de l'évolution de la technologie et des menaces émergent, à mesure que de nouvelles vulnérabilités sont découvertes. Les méthodes d'audit s'améliorent, lorsque les auditeurs internes adoptent une approche où les problématiques de contrôles des SI, à l'appui des objectifs de l'organisation sont une priorité absolue. Le management fournit les indicateurs de contrôle des SI et le reporting et les auditeurs internes se portent garants de leur validité et de leur qualité.

Le processus d'audit interne offre une démarche formelle pour traiter les contrôles des SI au sein du système global de contrôle interne. La figure 1 – La structure de l'audit des SI, scinde l'évaluation en une suite logique d'étapes.

Figure 1 – La structure de l'audit des SI

Évaluer les contrôles des SI	Compréhension des contrôles des SI	Contrôles – Gestion - Technique
		Généraux / Applicatifs
		Prévention, détection, correction
		Information - Sécurité
	Importance des contrôles des SI	Fiabilité et efficacité
		Avantage concurrentiel
		Législation et réglementation
	Rôles et responsabilités	Gouvernance
		Management
		Audit
	Approche par les risques	Analyse du risque
		Réponse au risque
		Contrôles élémentaires
	Surveillance et techniques	Cadre de contrôle
		Fréquence
	Évaluation	Méthodologies
		Interface avec le comité d'audit

Pour les contrôles des SI, l'auditeur interne doit tout d'abord disposer d'une bonne compréhension des concepts avant de pouvoir tirer les conclusions d'une évaluation des risques et des contrôles. Le RAI devrait surveiller les activités de formation et de réévaluation continues en fonction de l'émergence de nouvelles technologies, et de l'évolution des opportunités, usages, dépendances, stratégies, risques et besoins de l'entreprise.

6. Comprendre l'importance des contrôles des SI

Bien que ce GTAG traite exclusivement des risques et des contrôles liés aux SI, l'environnement de contrôle des SI (par exemple l'exemplarité du directeur des SI, le climat éthique, la philosophie du management et le style de management) est critique et devrait donc être évalué. Compte tenu du sujet de ce chapitre, le guide pratique de l'IIA, « Auditer l'environnement de contrôle », devrait être utilisé en complément.

Le COSO définit le contrôle interne comme « un processus mis en œuvre par la direction générale, le management, et autre personnel d'une organisation, destiné à fournir une assurance raisonnable quant à la réalisation des objectifs entrant dans les catégories suivantes :

- Efficacité et optimisation des opérations,
- Fiabilité des informations financières,
- Conformité aux lois et réglementations en vigueur. »

Les contrôles des SI englobent les processus qui procurent une assurance sur les données et les services informatiques et qui contribuent à contrôler et atténuer les risques découlant de l'usage des SI par une organisation. Il peut s'agir de politiques d'entreprise formalisées ou de leur mise en œuvre dans des programmes informatiques, de la protection des accès physiques à la capacité d'imputer des actions et des transactions aux utilisateurs, des validations automatiques ou encore des analyses de cohérence pour un grand volume de données.

Il n'est pas indispensable pour le RAI de « tout savoir » sur les contrôles des SI, incluant toute la gamme des contrôles ou toutes les subtilités techniques. Plusieurs contrôles relèvent de spécialistes qui gèrent des risques spécifiques associés aux différentes composantes des systèmes et de l'infrastructure de réseau.

6.1 *Les contrôles généraux et applicatifs des SI*

On peut classifier les contrôles de manière à en comprendre les objectifs et à savoir où ils s'insèrent au sein du système de contrôle interne (figure 2). La compréhension de ces classifications permet à celui qui analyse les contrôles et à l'auditeur de mieux connaître leur position au sein du système de contrôle et de répondre aux questions cruciales, telles : les contrôles détectifs sont-ils adéquats pour identifier les erreurs qui pourraient échapper aux contrôles préventifs ? Les contrôles correctifs sont-ils suffisants pour corriger les erreurs une fois celles-ci détectées ? Une classification courante des contrôles des SI, est de séparer les contrôles généraux des contrôles applicatifs. Pour avoir une définition plus complète sur les contrôles applicatifs, vous pouvez vous référer au GTAG 8 « L'audit des contrôles applicatifs ».

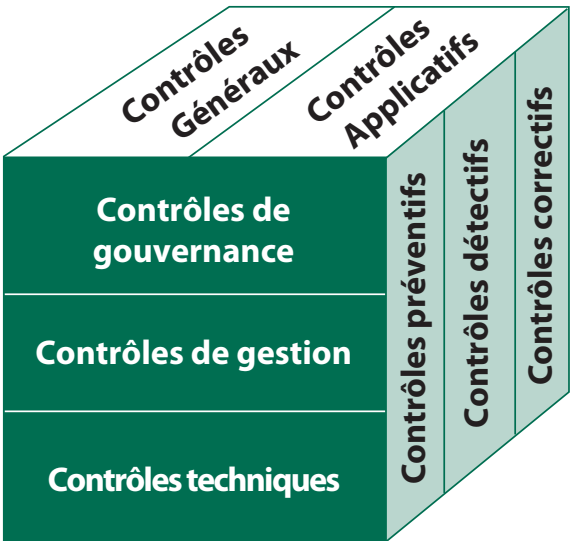

Figure 2 – Quelques classifications des contrôles

6.1.1 Les contrôles généraux

Les contrôles généraux s'appliquent à l'ensemble des composantes, processus et données d'une organisation ou d'un environnement système. Sans se limiter à ces domaines, les contrôles géné-

raux incluent la gouvernance des SI, la gestion des risques, la gestion des ressources, l'exploitation, le développement et la maintenance des applications, la gestion des utilisateurs, la sécurité logique, la sécurité physique, la gestion des changements des systèmes, la sauvegarde et la restauration de données, ou la continuité d'activité.

Certains contrôles généraux sont liés aux métiers (par exemple la séparation des fonctions ou l'organisation de la gouvernance), alors que d'autres sont plus techniques (tels que les contrôles des systèmes de logiciels, et les contrôles réseaux) et sont liés à l'infrastructure sous-jacente. Les contrôles généraux sont revus par l'audit interne car ils sont la base de l'environnement de contrôle des SI. Si les contrôles généraux sont peu fiables (par exemple le contrôle des accès et des changements), l'auditeur devra modifier son approche des tests pour les zones impactées.

6.1.2 Les contrôles applicatifs

Les contrôles applicatifs portent sur l'étendue des processus de l'organisation ou ses applications et incluent les contrôles au niveau des entrées, des traitements et des sorties des applications. Il s'agit, notamment, de la validation de données, de la séparation des tâches (par exemple : saisie et autorisation d'une transaction), balance des totaux de contrôle, journalisation des transactions et des rapports d'erreurs.

Le rôle d'un contrôle est primordial pour en évaluer la conception et l'efficacité. On peut généralement différencier les contrôles préventifs, détectifs et correctifs. Les contrôles préventifs permettent d'éviter la survenue d'erreurs, d'omissions ou d'incidents de sécurité. Il s'agit, par exemple, de simples règles de validation des données dès leur saisie, qui empêchent d'entrer des caractères alphabétiques dans des champs numériques, de contrôles d'accès grâce auxquels les données sensibles ou les ressources système deviennent inaccessibles aux individus non autorisés, ou encore de contrôles techniques dynamiques et complexes tels que les logiciels antivirus, les pare-feux et les systèmes anti-intrusion.

Les contrôles détectifs visent à repérer les erreurs ou les incidents qui échappent aux contrôles préventifs. Ainsi, un contrôle détectif peut identifier le nombre de comptes inactifs ou les comptes qui ont été signalés comme devant faire l'objet d'une surveillance pour déceler des activités suspectes. Les contrôles détectifs peuvent aussi prendre la forme d'une surveillance ou d'analyses visant à mettre au jour des activités ou des événements hors des limites autorisées ou des schémas connus pour certaines données, pouvant être sujet à une manipulation inadéquate. Pour les échanges de données sensibles, des contrôles détectifs peuvent indiquer si un message est corrompu ou si l'identité de l'expéditeur ne peut être authentifiée.

Les contrôles correctifs ont pour but de corriger les erreurs, omissions ou incidents une fois ceux-ci détectés. Il peut s'agir de la simple correction d'erreurs de saisie, de l'identification et la suppression d'utilisateurs ou de logiciels non autorisés, dans un système ou un réseau, ou encore de la reprise après un incident, une panne ou un sinistre.

Généralement, il est plus efficient de prévenir les erreurs ou de les détecter à un niveau aussi proche que possible de la source pour en simplifier la correction.

De nombreuses autres classifications des contrôles décrites dans ce guide peuvent être utiles pour en évaluer l'efficacité. Par exemple, les contrôles automatisés tendent à être plus fiables que les contrôles manuels, et les contrôles non discrétionnaires seront plus vraisemblablement appliqués de manière plus homogène que les contrôles discrétionnaires. Parmi les autres catégories possibles, citons les contrôles obligatoires, volontaires, complémentaires, compensatoires, redondants, continus, sur demande et déclenchés par des événements.

6.2 Les contrôles de la gouvernance, du management et techniques des SI

Une autre classification habituelle regroupe les contrôles en fonction du groupe chargé de veiller à leur mise en œuvre et de leur correcte actualisa-

tion. Afin d'évaluer les rôles et responsabilités, ce guide classe essentiellement les contrôles des SI en contrôles au niveau de la gouvernance, du management, du personnel technique ou au niveau des applications

Ce guide s'adresse en priorité aux deux premiers niveaux (gouvernance et management), bien qu'il puisse également être utile à un technicien de comprendre comment les contrôles sont mis en œuvre au niveau des infrastructures SI. Les contrôles techniques et applicatifs sont traités dans le cadre du GTAG 8 « Audit des contrôles applicatifs ».

6.2.1 Les contrôles de la gouvernance des SI

La responsabilité première de la surveillance du contrôle interne revient au Conseil, puisque c'est le dépositaire du cadre de gouvernance. Le contrôle des SI au niveau de la gouvernance implique de veiller à l'efficience de la gestion de l'information, à l'application des principes, politiques et processus de sécurité, et à vérifier que ce cadre fait en permanence l'objet de mesures de performance et de conformité. Ces contrôles sont associés aux concepts de gouvernance, lesquels sont guidés par les buts et objectifs de l'organisation et par les attentes des instances externes tels que les superviseurs.

6.2.2 Les contrôles du management

S'agissant du contrôle interne, la responsabilité du management consiste généralement à porter dans tous les domaines de l'organisation une attention particulière aux actifs critiques, aux données sensibles et aux fonctions opérationnelles. Le management doit s'assurer que les contrôles des SI nécessaires pour atteindre les objectifs que l'organisation s'est fixés sont mis en place et garantissent un processus de gouvernance fiable et continu. Le déploiement de ces contrôles résulte d'actions délibérées du management en réponse aux risques susceptibles d'affecter l'organisation, ses processus et ses actifs.

6.2.3 Les contrôles techniques

Les contrôles techniques sont souvent le socle des référentiels de contrôle du management. C'est pourquoi, si les contrôles techniques sont faibles, c'est le référentiel de contrôles dans sa globalité qui sera impacté. Par exemple, en assurant une protection contre les accès non autorisés et les intrusions, les contrôles techniques sont à la base de la fiabilité de l'intégrité des données, en apportant notamment des preuves de tous les changements et de leur authenticité. Ces contrôles sont différents selon les technologies en usage au sein de l'infrastructure SI de l'organisation. Ce sont, par exemple, des contrôles opérationnels de systèmes, les contrôles de bases de données, le cryptage et le contrôle des accès.

6.2.4 Les contrôles applicatifs

Comme déjà établi, les contrôles applicatifs portent sur l'ensemble des processus de l'organisation ou ses applications. Par nature techniques, les contrôles applicatifs peuvent également être non techniques en fonction de la zone de contrôle. Ils comprennent les contrôles des entrées, des traitements et des sorties. Le chapitre 6.3.7 de ce guide revient plus en détail sur le sujet.

6.3 Quels contrôles des SI ?

Les différents contrôles au sein d'une organisation peuvent être définis dans le cadre de la hiérarchie des contrôles des SI, allant des déclarations de principes généraux formulées par le management et avalisées par le Conseil, jusqu'aux mécanismes de contrôle spécifiques intégrés aux applications
La hiérarchie représentée à la figure 3 (page suivante) propose une approche logique descendante, à la fois lorsque l'on considère les contrôles à mettre en œuvre et aussi lorsque l'on définit sur quels aspects concentrer les ressources d'audit durant l'examen de l'environnement d'exploitation des SI. Les différents éléments de contrôle placés dans cette hiérarchie ne sont pas mutuellement exclusifs ; ils sont tous reliés les uns aux

autres, se chevauchent et se confondent souvent. Nous décrivons ci-dessous un certain nombre de contrôles.

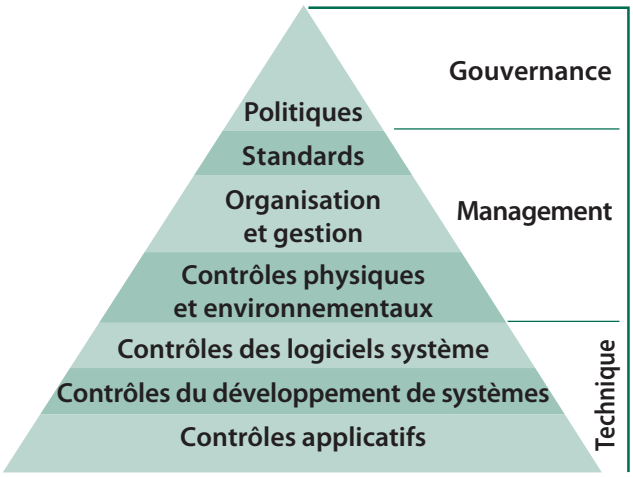

Figure 3 – Les contrôles des SI

6.3.1 Règles et procédures

Toutes les organisations doivent définir leurs buts et objectifs à travers des plans stratégiques et des politiques. En l'absence de politiques et de règles formalisées pour le management, les organisations, manquant d'orientations à suivre, peuvent devenir inefficientes.

Les SI étant essentiels pour la plupart des organisations, il faut que les principes qui régissent tous les aspects des SI soient clairement définis, et approuvés par la direction générale, que le Conseil les avalise et qu'ils soient communiqués au personnel. En fonction de la taille de l'organisation et de son niveau d'informatisation, il peut être parfois nécessaire de formuler de nombreuses politiques différentes. Pour les organisations plus petites, une seule politique peut suffire, tant qu'elle couvre tous les aspects concernés. Les organisations plus grandes auront souvent besoin de politiques plus détaillées et plus spécifiques.

Les politiques SI peuvent par exemple inclure :

- Une politique générale sur le niveau de sécurité et le respect de la vie privée pour l'ensemble de l'organisation. Cette politique doit être cohérente avec l'ensemble des législations nationales et internationales en vigueur et doit spécifier le niveau de contrôle et de sécurité requis en fonction du niveau de sensibilité du système et des données traitées.
- Une politique sur la classification des données et les droits d'accès applicables selon celle-ci. Elle doit également définir les limitations quant à l'utilisation de ces données par les personnes habilitées.
- Une définition des concepts de propriété des systèmes et des données, ainsi que de l'habilitation nécessaire pour créer, modifier ou supprimer les données. Il peut s'agir d'une politique générale qui définit dans quelles mesures les utilisateurs peuvent créer leurs propres applications.
- Des politiques de ressources humaines qui définissent les conditions de travail dans les domaines sensibles et en vérifient la bonne application. Il peut s'agir d'examiner en détail les informations concernant des candidats à l'embauche avant de les accueillir dans l'organisation, et de faire signer aux employés des accords par lesquels ils acceptent la responsabilité pour le niveau de contrôle, de sécurité et de confidentialité requis. Typiquement, cette politique peut également détailler les procédures disciplinaires correspondantes.
- La définition des exigences en matière de plans de continuité d'activité, en veillant à ce que tous les aspects de l'activité, soient pris en compte dans l'éventualité d'une panne ou d'un sinistre.

Cette liste n'est bien sûr pas exhaustive.

6.3.2 Normes

L'organisation devrait avoir un projet SI qui supporte toute sa stratégie et fixe les règles des normes et politiques SI[1].

[1] *Le Cadre de Référence International des pratiques professionnelles de l'audit interne de l'IIA s'assure que l'audit interne évalue la stratégie SI. Selon la norme 2110.A2 « L'audit interne doit évaluer si la gouvernance des systèmes d'information de l'organisation soutient la stratégie et les objectifs de l'organisation. »*

Les normes visent à définir des méthodes de travail qui permettent la réalisation des objectifs de l'organisation. De surcroît, l'adoption et l'utilisation de normes promeuvent l'efficience, et assurent la cohérence de l'ensemble de l'environnement d'exploitation SI.
Les grandes organisations qui disposent de ressources importantes peuvent tout à fait concevoir leurs propres normes. Mais, les petites organisations ont rarement les ressources suffisantes pour le faire. Il existe de nombreuses sources d'informations sur les normes et les bonnes pratiques. Par exemple, la DSI devrait prendre en compte :

- Les **procédures de développement des systèmes**. Lorsque des organisations développent leurs propres applications, des normes définissent les procédures de conception, développement, test, mise en œuvre et maintenance des systèmes et programmes. Si elles externalisent le développement d'applications ou acquièrent des systèmes auprès d'éditeurs, le RAI doit s'assurer que des accords exigent du fournisseur qu'il applique des normes qui sont conformes à celles de l'organisation ou qui soient acceptables par cette dernière.
- La **configuration de logiciels**. Parce que les logiciels procurent une part importante du contrôle de l'environnement SI, les normes relatives à la configuration sécurisée de systèmes sont de plus en plus largement acceptées par les organisations et fournisseurs de technologies leaders. La configuration des produits tels que les systèmes d'exploitation, les logiciels de réseau et les systèmes de gestion de bases de données peut soit renforcer leur sécurité, soit créer des vulnérabilités qui risquent d'être exploitées à mauvais escient.
- Les **contrôles applicatifs**. Toutes les applications qui supportent les activités métiers doivent être contrôlées. Pour toutes les applications que l'organisation développe ou acquiert, des normes doivent définir les types de contrôle à mettre impérativement en place tout le long des processus métiers, ainsi que les contrôles spécifiques aux processus et données sensibles.
- La **structure des données**. Si l'on dispose de définitions de données homogènes dans la totalité des applications, des systèmes distribués peuvent accéder sans difficulté aux données, et des contrôles de sécurité peuvent être mis en place uniformément sur toutes les données à caractère personnel et autres données sensibles.
- La **documentation**. Des normes doivent spécifier le niveau de détail minimal de documentation requis pour chaque application ou implémentation informatique, ainsi que pour les différentes catégories d'applications, de procédures et de centres de traitement.

Comme les politiques, les normes formalisées doivent être approuvées par le management, et accessibles à tous ceux qui ont à les appliquer.

6.3.3 Organisation et management

L'organisation et le management jouent un rôle clé dans l'ensemble du système de contrôle des SI, comme dans tous les aspects de la vie d'une organisation. Une structure adéquate permet la définition de rattachements hiérarchiques et de responsabilité ainsi que la mise en place de systèmes de contrôle efficaces. Les principaux contrôles clés qui sont habituellement mis en place sont la séparation des tâches incompatibles, les contrôles financiers et la gestion du changement.

6.3.3.1 Séparation des tâches

La séparation des tâches est un élément crucial de nombreux contrôles. Une organisation doit être structurée de sorte que tous les aspects du traitement des données ne reposent jamais sur une seule personne. Les fonctions d'émission, d'autorisation, de saisie, de traitement et de vérification des données doivent être séparées afin qu'aucun individu ne puisse être à l'origine d'une erreur ou d'une omission ou de toute autre irrégularité et l'autoriser et/ou en masquer les preuves. Les contrôles de séparation des tâches concernant les applications sont mis en place par l'octroi d'accès privilégiés en fonction des exigences du poste en

termes de traitement et d'accès aux données.
La séparation traditionnelle des tâches dans le domaine informatique répond à la distinction entre développement de système et exploitation des SI. L'exploitation des SI doit assurer le fonctionnement des systèmes de production, sauf pour ce qui est du déploiement du changement, et avoir peu voire aucune responsabilité, dans le processus de développement. Ce contrôle prévoit des restrictions qui empêchent les exploitants d'accéder aux programmes, systèmes ou données de production ou de les modifier. De même, les développeurs doivent avoir peu de contacts avec les systèmes de production. On obtiendra une séparation des tâches adéquate en assignant des rôles différents lors des processus de mise en production et de changement. Dans les grandes organisations, il faut procéder de la même manière pour de nombreuses fonctions si l'on veut que la séparation des tâches soit adéquate.

6.3.3.2 Contrôles financiers

Étant donné que les organisations réalisent des investissements considérables dans les SI, des contrôles d'ordre budgétaire et financier sont nécessaires pour s'assurer qu'ils aboutissent au retour sur investissement ou aux économies annoncés. Il convient de mettre en place des procédures de gestion permettant de recueillir, d'analyser et de rendre compte de ces aspects. Malheureusement, les évolutions des SI induisent souvent des dépassements de coût massifs et ne se traduisent pas par les économies ou les revenus attendus, en raison d'estimations erronées ou d'une planification insuffisante.

6.3.3.3 Gestion du changement

Les procédures de gestion du changement[1] s'assurent que les modifications apportées à l'environnement de SI, aux logiciels, aux applications et aux données doivent permettre de respecter une bonne séparation des tâches, d'assurer le bon fonctionnement des changements, d'empêcher l'exploitation de ces changements à des fins frauduleuses. Une faiblesse dans la gestion du changement pourrait sérieusement impacter le système et le service disponibles.

6.3.4 Contrôles physiques et environnementaux

Les équipements informatiques représentent un investissement considérable pour de nombreuses organisations. Il faut donc les protéger des pertes ou dégradations accidentelles ou délibérées. Les contrôles physiques et environnementaux, initialement mis au point pour les grands centres de traitement informatique qui hébergent des mainframes, sont tout aussi importants dans le monde des architectures client-serveur et les systèmes Web. Bien que les équipements communément utilisés de nos jours soient conçus pour être simples d'utilisation dans un environnement de bureau normal, leur valeur pour l'organisation, le coût et la vulnérabilité des applications qui font fonctionner les processus de l'organisation peuvent être significatifs.
Tous les équipements doivent être protégés, y compris les serveurs et les postes de travail qui permettent au personnel d'accéder aux applications. Parmi les contrôles physiques et environnementaux, citons :

- L'installation des serveurs dans des locaux verrouillés et à accès restreint.
- La limitation de l'accès aux serveurs à des personnes autorisés.
- La mise en place de dispositifs de détection incendie et d'extincteurs.
- L'installation des équipements, applications et données sensibles à distance des risques environnementaux, par exemple loin de zones inondables, des couloirs aériens ou de lieux de stockage de liquides inflammables.

Lorsque l'on s'intéresse à la sécurité physique et environnementale, il convient également d'envisager le plan de reprise après un sinistre[2].
Que faire en cas d'incendie ou d'inondation, ou si d'autres menaces se présentent ? Comment l'organisation doit-elle procéder pour redémarrer l'activité et les installations et services informa-

[1] *GTAG 2 : Contrôles de la gestion du changement et des patchs : un facteur clé de la réussite pour toute organisation (2ème éd.).*
[1] *GTAG 10 « Gestion de la continuité d'activité ».*

tiques rattachés, afin que le fonctionnement normal se poursuive avec des incidences aussi faibles que possible sur les activités habituelles ? Ce type de planification ne se contente pas de proposer des capacités de traitement informatique de secours ou une sauvegarde régulière des données de production. Il doit envisager la logistique et la coordination nécessaires pour couvrir tout le champ de l'activité. Enfin, l'expérience montre, à chaque fois, qu'un plan de secours, qui n'a pas été testé avec succès, ne sera pas fiable en situation réelle.

6.3.5 Contrôles des logiciels systèmes

Les logiciels système permettent aux applications et aux utilisateurs d'exploiter l'équipement informatique. Il s'agit de systèmes d'exploitation comme Windows, UNIX ou Linux, de logiciels de gestion de réseau et de transmission, de pare-feux, d'antivirus ou encore de système de gestion de bases de données (SGBD) tels qu'Oracle et DB2.
Les spécialistes de l'audit des SI doivent évaluer ces contrôles. Il est peu vraisemblable que les petites organisations aient des ressources suffisantes pour employer ce type de spécialistes, ainsi elles doivent envisager d'externaliser ce travail. Les auditeurs informatiques, soit employés directement ou intervenant en sous-traitance, doivent disposer de connaissances très spécifiques. Ils acquièrent l'essentiel de ce savoir par l'expérience, mais il leur faut constamment mettre à jour leurs connaissances afin qu'elles restent actualisées et utiles.
Les systèmes de logiciels peuvent s'avérer extrêmement complexes et s'appliquer à différents éléments et à des appareils au sein des systèmes et de l'environnement réseau. Le logiciel peut être configuré pour répondre à des besoins très spécifiques et donc avoir besoin d'un niveau élevé de spécialisation pour une maintenance sécurisée. Bien que les systèmes de certaines applications possèdent leur propre système de contrôle des accès et pourraient alors fournir un accès à des utilisateurs non autorisés pour rentrer dans le système, les paramétrages techniques permettent un contrôle des accès logiques aux applications. Ils permettent également de renforcer la séparation des tâches, de générer des pistes d'audit et s'appliquer aux contrôles d'intégrité des données à travers les listes de contrôles d'accès, des filtres et des connexions.
Voici quelques-uns des contrôles techniques clés que l'on doit s'attendre à trouver dans un environnement de SI bien géré :

- Les droits d'accès sont attribués et contrôlés conformément à la politique énoncée par l'organisation.
- Les principes de séparation des tâches sont respectés grâce à des contrôles logiciels et d'autres contrôles de configuration.
- Des évaluations et des actions de prévention et de détection des intrusions et des vulnérabilités[1] sont en place et suivies en continu.
- Des tests d'intrusion sont régulièrement réalisés.
- Des services de chiffrement sont mis en œuvre lorsque la confidentialité est explicitement requise.
- Des procédures de gestion des changements, y compris la gestion des patchs, sont en place, si bien que les changements et les patchs sont appliqués aux logiciels, systèmes, composants réseau et données selon une procédure étroitement encadrée[2].

6.3.6 Contrôles de l'acquisition et de développement des systèmes

Les organisations adoptent rarement une méthodologie unique pour tous les projets de développement de systèmes. La méthodologie retenue doit correspondre au contexte particulier à chaque projet. Les auditeurs informatiques doivent déterminer si oui ou non l'organisation développe ou acquiert des applications selon une méthode encadrée, qui prévoit ensuite des contrôles efficaces sur et au sein des applications et données traitées. Par l'examen des procédures de développement des

[1] *GTAG 6 « Gérer et auditer les vulnérabilités des technologies de l'information ».*
[1] *GTAG 2 « Contrôles de la gestion du changement et des patchs : un facteur clé de la réussite pour toute organisation (2ème éd.) ».*

applications, l'auditeur peut obtenir l'assurance que les contrôles applicatifs sont adéquats. Certains points de contrôle de base doivent être traités dans toutes les activités d'acquisition et de développement de systèmes. Par exemple :

- Les besoins des utilisateurs doivent être formalisés, et leur satisfaction mesurée.
- La conception des systèmes doit suivre une procédure formelle qui permet de s'assurer que les besoins des utilisateurs et les contrôles sont bien intégrés dans le système.
- Le développement des systèmes doit être mené de manière structurée, afin que les besoins et les spécifications requis soient bien pris en compte dans le produit final.
- Les tests doivent vérifier que les différentes composantes du système opèrent de la façon requise, que les interfaces fonctionnent comme prévu, que les utilisateurs participent au processus de test et que les fonctionnalités attendues sont bien présentes.
- Les procédures de maintenance des applications doivent permettre de s'assurer que tous les changements apportés aux applications répondent à un schéma de contrôle homogène. La gestion des changements doit faire l'objet de procédures structurées de validation de l'assurance.

Si le développement est externalisé, les prestataires doivent se voir imposer, par contrat, des contrôles similaires. Les techniques et contrôles de gestion de projet devraient faire partie intégrante du processus de développement, que celui-ci soit réalisé en interne ou externalisé. La direction générale doit savoir si les projets respectent les délais, ne dépassent pas le budget et si les ressources sont utilisées avec efficience. Des remontées d'information sur les projets doivent permettre à la direction générale d'avoir une compréhension de l'état d'avancement des projets de développement et d'éviter d'avoir de mauvaises surprises lors de la mise en service du produit final[1]. Le GTAG 12 « Auditer les projets informatiques » évoque également l'évaluation des projets d'acquisition ou de développement.

6.3.7 Contrôles applicatifs[2]

Les points de contrôle interne portant sur les applications veillent à ce que :

- Toutes les données saisies soient exactes, complètes, autorisées et correctes.
- Toutes les données soient traitées comme prévu.
- Toutes les données stockées soient exactes et complètes.
- Tous les résultats soient exacts et complets.
- Le traitement des données fasse l'objet de traces (logs) depuis la saisie jusqu'au stockage et à la production de données de sortie.

L'examen des contrôles d'application a toujours constitué le domaine des auditeurs informatiques. Cependant, ce type de contrôles représentant désormais une composante essentielle de la maîtrise des activités, tous les auditeurs internes devraient en faire une priorité.
Différents types de contrôles courants devraient exister dans chaque application :

- **Les contrôles des données d'entrée :** ils servent essentiellement à vérifier l'intégrité des données saisies dans une application, qu'elles soient saisies directement par les utilisateurs, à distance par un partenaire ou à travers une application Web. Une vérification des entrées permet de s'assurer qu'elles respectent les paramètres spécifiés.
- **Les contrôles du traitement :** ils procurent un moyen automatisé de s'assurer que le traitement est complet, exact et autorisé.
- **Les contrôles des données de sortie :** ils portent sur ce qui est fait des données. Ils doivent comparer les résultats obtenus aux résultats attendus, et les vérifier par rapport à ce qui a été saisi.
- **Les contrôles d'intégrité :** ils peuvent s'appliquer de façon permanente sur les données en cours de traitement et/ou stockées, afin de s'assurer qu'elles restent cohérentes et exactes.

---

[1] *GTAG 14 « L'audit des applications développées par les utilisateurs ».*
[1] *GTAG 8 « Audit des contrôles applicatifs ».*

- **La traçabilité :** le fait de traiter l'historique des contrôles, ce qu'on appelle souvent une piste d'audit, permet au management de suivre les transactions depuis la source jusqu'au résultat final ou de remonter à partir des résultats jusqu'aux transactions et les événements enregistrés qui les ont générés. Ces contrôles doivent permettre de surveiller l'efficacité de l'ensemble des contrôles et de déceler les erreurs le plus en amont possible.

6.4 Sécurité informatique

La sécurité informatique[1] fait partie intégrante des contrôles des SI. Elle s'applique à la fois à l'infrastructure et aux données, et c'est sur elle que repose la fiabilité des autres contrôles des SI, à l'exception de ceux ayant trait aux aspects financiers des SI (par exemple le retour sur investissement, les contrôles budgétaires) et de quelques contrôles de gestion de projet. Les composantes généralement acceptées de la sécurité informatique sont :

- La **confidentialité :** les données confidentielles ne doivent être divulguées que lorsque c'est nécessaire, et doivent être protégées contre toute interception ou communication non autorisée. La confidentialité a également trait au respect de la vie privée et des données personnelles.
- L'**intégrité :** l'intégrité des données désigne des données correctes et complètes. Elle est particulièrement importante pour la fiabilité du traitement de données financières et les communications financières.
- La **disponibilité :** les données doivent être accessibles à l'organisation, à ses clients et partenaires au moment, à l'endroit et de la manière requise. La disponibilité porte également sur la capacité de redémarrage des SI après une perte, une panne ou la corruption de données et de services des SI, ou encore après un sinistre majeur à l'emplacement où les données étaient situées.

6.5 Cadre de contrôle des SI

Les organisations utilisent les SI depuis plus de 50 ans et, sur cette période, les contrôles n'ont pas toujours constitué une caractéristique par défaut des nouveaux matériels ou logiciels. L'élaboration et la mise en place de contrôles arrivent généralement après que l'on ait décelé une vulnérabilité dans le système ou des menaces qui exploitent ces vulnérabilités. En outre, les contrôles des SI ne sont pas définis dans des normes universellement reconnues applicables à tous les systèmes ou à toutes les organisations qui les utilisent.
Un cadre de contrôle permet de structurer la typologie et l'identification des contrôles pour sécuriser l'environnement SI. Ce cadre peut être formel ou informel. Une approche formelle sera plus satisfaisante pour répondre aux différents régulateurs ou aux exigences légales auxquels sont soumises les organisations. Toutes les parties concernées, notamment les propriétaires des processus métiers et les fonctions qui mettent en œuvre les contrôles, doivent être impliquées dans la définition ou l'élaboration du cadre de contrôle. Ce cadre de contrôle devrait être appliqué et utilisé par l'ensemble de l'organisation.

[1] *GTAG 15 « La gouvernance de la sécurité de l'information ».*

7. Compétences et savoir-faire dans le domaine de l'audit des SI

Selon le CRIPP, les auditeurs internes doivent appliquer et veiller au respect de quatre principes : intégrité, objectivité, confidentialité et compétence. Le principe de compétence impose aux auditeurs internes de s'engager uniquement dans des travaux pour lesquels ils ont les connaissances, le savoir-faire et l'expérience nécessaires. En outre, la norme de qualification « 1210 : Compétence » de l'IIA, précise que « Les auditeurs internes doivent posséder les connaissances, le savoir-faire et les autres compétences nécessaires à l'exercice de leurs responsabilités individuelles. L'équipe d'audit interne doit collectivement posséder ou acquérir les connaissances, le savoir-faire et les autres compétences nécessaires à l'exercice de ses responsabilités. »
Le RAI doit obtenir l'avis et l'assistance de personnes qualifiées si les auditeurs internes ne possèdent pas les connaissances, le savoir-faire ou les autres compétences nécessaires pour s'acquitter de tout ou partie de la mission. L'IIA fournit un cadre de référence intitulé *Integrated Competency Framework* qui aide à identifier les compétences nécessaires à l'activité d'audit interne. Cette approche relie les risques opérationnels identifiés aux processus des SI auxquels ils se rapportent. Le RAI devrait donc savoir quel type et quel niveau de compétences et de savoir-faire en matière de SI sont requis pour auditer l'efficacité des contrôles sur les risques opérationnels identifiés. Le tableau ci-après donne quelques exemples de liens entre risques opérationnels et contrôles des SI, et de savoir-faire / compétences requis pour exécuter l'audit.

Risque métiers	Contrôles des SI	Savoir-faire et compétences en matière de SI
Gestion de la sécurité informatique	Contrôle de la sécurité logique efficace	Administration de la sécurité ; contrôles d'accès au niveau du réseau, du système opérationnel, des bases de données et des applications
Interruption critique de l'activité	Garantir la disponibilité des applications métiers critiques	Plans de continuité d'activité et plan de secours pour les installations informatiques (notamment l'infrastructure réseau, les systèmes opérationnels, les bases de données et les applications)
Informations financières et opérationnelles inexactes et incomplètes	Sécuriser la confidentialité et la disponibilité des données	Contrôles applicatifs, contrôles des changements et des cycles de vie du développement logiciel (SDLC)

Si l'audit interne ne possède pas les compétences et le savoir-faire requis dans le domaine des SI, le RAI peut faire appel à un prestataire externe pour soutenir ou compléter l'équipe interne (externalisation ou ressources externes partagées).[1]

[1] *Voir la Modalité pratique d'application « 1210.A1-1: Recours à des prestataires externes » de l'IIA.*

8. Utilisation du cadre de contrôle

Chaque organisation devrait examiner les cadres de contrôle existants et déterminer lesquels (ou quelles parties) répondent le mieux à ses besoins. Le choix ou l'élaboration d'un cadre de contrôle doit associer tout le personnel de l'organisation ayant une responsabilité directe vis-à-vis des contrôles. L'audit interne évaluera l'adéquation du cadre et l'utilisera pour la planification et l'exécution des travaux d'audit interne.

Le RAI doit avoir une connaissance globale des risques liés aux SI pour juger de l'efficacité et de l'adéquation des contrôles des SI. Il élabore le plan d'audit interne et affecte les ressources dans les domaines et aux problématiques qui appellent une attention particulière en raison de leur niveau de risque intrinsèque. L'analyse et l'évaluation des risques ne peuvent pas être réalisées une fois pour toutes, surtout si elles s'appliquent aux SI. La technologie évolue constamment et rapidement, de même que les risques et menaces qui y sont associés. La classification des contrôles des SI d'après leur positionnement, objectif et fonction au sein de l'organisation peut se révéler utile pour en évaluer leur pertinence et leur adéquation, et pour juger si le système de contrôle interne est approprié. La connaissance de la gamme des contrôles des SI disponibles, des raisons d'être de ces contrôles ainsi que des rôles et responsabilités au sein de l'organisation permet des analyses et des évaluations complètes de risques. Lorsque l'on juge de l'efficacité des contrôles, il est également utile de savoir si ces derniers sont obligatoires ou facultatifs, discrétionnaires ou non, manuels ou automatisés, clés ou secondaires, et si le management peut avoir la possibilité de les outrepasser.

Enfin, l'évaluation des contrôles des SI suppose de sélectionner des contrôles clés qui seront testés, d'en évaluer les résultats, et de déterminer si les éléments de preuves permettent de déceler des faiblesses significatives. La liste de vérification présentée en annexe peut aider à s'assurer que toutes les problématiques pertinentes ont été prises en considération lors de la planification et du choix de l'orientation donnée aux évaluations d'audit interne sur les contrôles des SI. Plusieurs référentiels et approches peuvent aider le RAI et d'autres managers à définir les besoins de contrôles des SI. Cependant, les organisations doivent étudier suffisamment de cadres de référence pour savoir lequel correspond le mieux à leurs besoins et à leur culture.

8.1 Techniques d'audit assisté par ordinateur et analyse des données

Les RAI devraient envisager d'utiliser des techniques d'audit assisté par ordinateur - notamment des outils d'analyse des données - pour obtenir une vision réaliste de l'environnement des risques liés aux SI et pour identifier les anomalies potentielles. Dans un contexte où les organisations et les activités d'audit interne doivent en faire plus avec des moyens réduits, l'analyse des données permet aux RAI d'exploiter les informations disponibles dans l'ensemble de l'organisation et d'identifier des domaines nécessitant potentiellement une évaluation des risques ou un audit. L'analyse des données peut également représenter pour le RAI une approche pour évaluer en continu l'efficacité opérationnelle des contrôles et pour analyser les indicateurs des risques émergents. Les outils existants d'analyse des données accroissent les possibilités de l'audit des informations et l'efficience du traitement de volumes de données plus importants. Toutefois, les RAI sont confrontés à des difficultés importantes : ils doivent obtenir le savoir-faire technique, accéder aux outils d'analyse des données, exploiter les outils de *reporting* / d'extraction des données, accéder aux sources de données et élaborer une stratégie axée sur les risques organisationnels les plus élevés.
L'audit continu est semblable à la surveillance continue, les données étant analysées ou évaluées en continu par l'audit interne. La surveillance continue relève de la responsabilité et de la fonction du management. L'audit interne peut tester, revoir ou exploiter l'utilisation de la surveillance

continue. Pour de plus amples informations, voir le GTAG 3 de l'IIA « Audit continu : répercussions sur l'assurance, le pilotage et l'évaluation des risques ».

8.2 Recours à l'évaluation automatisée des risques

Le RAI peut estimer que pour renforcer son évaluation des risques, il doit procéder à une cotation ou à une évaluation détaillée des risques. Certains outils permettent également l'automatisation du processus d'analyse des risques. Ces outils permettent d'établir une cotation des risques, de préciser leur impact et d'en estimer la probabilité, entre autres facteurs. Grâce à l'automatisation de l'évaluation des risques, il est possible de comparer et de hiérarchiser les risques. Le recensement des facteurs de risque inhérents et résiduels permet au RAI de fournir des informations résumées telles que des cartographies des risques ou des profils de risques correspondant au profil de risque de l'organisation. L'automatisation de la gestion de l'audit interne est un sujet important en soi. L'automatisation du processus d'évaluation des risques (par exemple le recours à des outils pour permettre au management d'enregistrer les cotations du risque) représente une opportunité.

8.3 Reporting des contrôles des SI

Les RAI doivent communiquer aux principales parties prenantes - par exemple le Comité d'audit, le comité exécutif, les instances de réglementation, les auditeurs externes ou le directeur des SI - les résultats des missions d'assurance. Les RAI peuvent utiliser différents formats de rapport, et les approches peuvent aller des mises à jour aux tableaux de bord, en passant par des présentations à huis-clos à la direction générale.

Une approche consiste à commencer par actualiser l'évaluation. Le RAI devrait tout d'abord déterminer le niveau de risque inhérent à certains processus clés des SI. Par exemple, le RAI peut indiquer et vérifier avec le directeur des SI ou les principales parties prenantes des SI le risque inhérent au développement, à l'exploitation, au plan de continuité des activités, au réseau, à la sécurité informatique et à la gestion du changement. Le risque inhérent dépend souvent de la stratégie et de l'organisation des SI. Certaines organisations des SI peuvent être externalisées, centralisées ou décentralisées. Les actualisations peuvent prendre la forme de projets d'audit dans différents domaines fonctionnels des SI, et peuvent englober des constats ou des problématiques importants.

Contribution de l'audit aux contrôles des SI

Au cours des dernières décennies, on s'est, à plusieurs reprises, interrogé, en particulier lorsque la direction générale et les auditeurs s'accordaient à dire que ces derniers pouvaient être source de valeur ajoutée pour l'organisation en apportant aux processus de développement leur expertise en matière de contrôles ; cette démarche permettait de veiller à ce que des contrôles adéquats soient intégrés aux nouveaux systèmes, au lieu de n'y ajouter des contrôles qu'après que l'audit ait détecté des failles. Ces activités ont coïncidé avec les avancées dans l'autoévaluation des contrôles et des risques dans le monde de l'audit. Les missions de conseil et l'approche d'audit fondée sur les risques se sont généralisées. A partir des années 1990 et après, on a prêté davantage attention à la gestion de la sécurité informatique, à mesure que des cyber-attaques de plus en plus graves se multipliaient. Ces événements ont contribué à façonner le rôle de l'auditeur informatique et la prise de conscience des organisations de l'importance d'une gestion efficace de la sécurité informatique.

L'état d'avancement des recommandations d'audit pourrait également faire partie de l'actualisation sur les SI.

Une autre approche consiste à utiliser un tableau de bord aligné avec le tableau de bord *(Balanced Scorecard)* utilisé par le directeur des SI pour le *reporting* de la stratégie et des activités informatiques. Le *Balanced Scorecard* Institute donne un modèle qui considère l'activité informatique selon quatre axes : financier, client, processus métiers internes, apprentissage organisationnel et développement. Lorsque le RAI rend compte des SI dans le cadre du *reporting* régulier au Conseil, au Comité d'audit ou à la direction générale, le rapport devrait couvrir généralement des problématiques liées aux incidents affectant la sécurité informatique, les anomalies en matière de gestion du changement, l'état d'avancement de projets, le *reporting* des incidents d'exploitation, les dépenses d'investissement, et d'autres indicateurs mesurant les principaux risques et l'évaluation des contrôles des SI. Ce type d'approche permet une appréhension intégrée et exhaustive de tous les risques et contrôles – métier et SI – dans un seul format.

Il arrive que le RAI ait besoin d'organiser des réunions en comité restreint. Ce type de *reporting* concerne généralement les problématiques importantes. Il peut s'agir par exemple de l'incapacité de l'équipe d'audit interne à obtenir des données demandées malgré des tentatives répétées, de collaborateurs clés de la DSI ne fournissant pas des informations complètes, ou des responsables informatiques qui excluent l'auditeur interne des discussions importantes, de comités de pilotage (qui ne le convie pas). L'absence de soutien du directeur des SI peut également constituer une difficulté nécessitant une réunion. Cette « exemplarité » peut instaurer une culture inadéquate, voire bloquer les mesures correctrices ou permettre aux principaux contrôles des SI de fonctionner sans surveillance.

9. Conclusion

L'évaluation des risques et des contrôles des SI représente – pour les nouveaux RAI comme pour les plus expérimentés – l'une des premières étapes vers la compréhension de l'environnement des SI et de son importance dans la gestion des risques de l'organisation. La lecture et l'application des recommandations de ce GTAG permettront aux RAI et aux auditeurs internes de mieux comprendre les risques des SI et les contrôles applicables. Le RAI pourra ensuite animer des discussions sur les risques et les contrôles des SI avec les principales parties prenantes.

L'étape suivante, l'évaluation et la compréhension de la gouvernance des SI, permet au RAI d'identifier les responsabilités au sein des SI et de déterminer comment la DSI, en coopération avec la direction générale, déploie la stratégie des SI. Dans ce contexte, les RAI devraient garder à l'esprit les dispositions de la Norme 2110.A2 de l'IIA concernant « l'évaluation de la gouvernance des SI ». La Section 3 (Parties prenantes internes et responsabilités des SI) de ce document résume de façon utile les principaux rôles et responsabilités.

Une fois que le RAI évalue la gouvernance des SI, l'étape suivante logique du processus est celle de l'analyse des risques liés aux SI. Malheureusement, il n'existe pas de liste de vérification universelle pour analyser les risques liés aux SI. Chaque organisation - selon les spécificités de ses métiers ou de sa taille - fonctionne avec des infrastructures, des applications et des interfaces technologiques différentes, et utilise des politiques différentes pour mener à bien sa stratégie des SI. Le RAI devrait effectuer une analyse des risques en utilisant une méthodologie structurée, telle que celle exposée dans la norme ISO 31000 « Management du risque » ou COSO II, et exploiter les connaissances des principaux responsables des SI (par exemple le directeur des SI et autres directeurs) dans le contexte des risques globaux inhérents à l'organisation. Le développement de relations de confiance solides favorisera la transparence lors de l'analyse des risques inhérents et résiduels.

Il existe de nombreux modèles et approches pour analyser les risques liés aux SI, et le RAI devrait sélectionner ceux qui correspondent le mieux à son organisation. Plusieurs rôles et fonctions clés des SI sont détaillés à la Section 6 (Comprendre l'importance des contrôles des SI) de ce document. Le RAI note les niveaux de risque liés aux SI et détermine les éléments devant être intégrés au plan d'audit général.
À partir du plan d'audit général, le RAI doit identifier et évaluer le savoir-faire et les compétences techniques nécessaires. Il peut s'inspirer de la *GAIT Methodology* de l'IIA lorsqu'il utilise une approche descendante basée sur les risques. Certaines spécialisations peuvent toutefois être coûteuses à déployer à titre permanent. Les RAI peuvent exploiter des savoir-faire acquis en interne ou recrutés, ou faire appel à des prestataires externes. S'appuyer sur des ressources externes permet aux organisations de toutes tailles de bénéficier d'une expertise ainsi que d'une visibilité sur les tendances les plus récentes et leur risque.

L'évaluation des risques et des contrôles des SI s'appuie sur un plan réfléchi et organisé. Les RAI devraient prévoir suffisamment de temps et de ressources qualifiées pour adopter une approche professionnelle et établir un processus pérenne d'analyse continue.

Auteurs et réviseurs

Auteurs
Steve Mar, CFSA, CISA
Rune Johannessen, CIA, CCSA, CISA
Stephen Coates, CIA, CGAP, CISA
Karine Wegrzynowicz, CIA
Thomas Andreesen, CISA, CRISC

Réviseurs
Steve Hunt, CIA
Steve Jameson, CIA, CCSA, CFSA, CRMA

Autres contributeurs
Dragon Tai, CIA, CCSA

Réviseurs en français
Béatrice Ki-Zerbo, CIA
Alain Rogulski, CIA

Annexe : Liste de vérification du Cadre de contrôles des SI

Les RAI peuvent utiliser cette liste de vérification pour examiner leur cadre de contrôle des SI afin de vérifier que l'organisation a pris en compte tous les éléments de contrôle. Cette liste peut les aider à comprendre les problèmes et à planifier une mission d'audit interne couvrant l'intégralité des champs de vérification.

Actions	Questions
1. Déterminer l'environnement de contrôle des SI de l'organisation, notamment : a. Ses valeurs. b. Sa philosophie. c. Son style de management. d. Sa connaissance des SI. e. Son organisation. f. Ses politiques. g. Ses normes.	• Existe-t-il des politiques et des normes d'entreprise expliquant la nécessité des contrôles des SI ?
2. Identifier la législation et la réglementation qui ont des conséquences sur les contrôles des SI : a. La gouvernance. b. La communication financière. c. La protection des données. d. Le respect des règles.	• Quelles sont les lois en vigueur ayant des conséquences sur les besoins de contrôle des SI ? • La direction générale a-t-elle pris des mesures en vue de respecter cette législation ?
3. Identifier les rôles et les responsabilités relatifs au contrôle des SI pour : a. Le conseil d'administration. i. Le comité d'audit. ii. Le comité de gestion des risques. iii. Le comité de gouvernance. iv. Le comité financier. b. Le management. i. Le directeur général. ii. Le directeur financier et le contrôleur de gestion. iii. Le directeur des SI. iv. Le directeur de la sécurité / sûreté. v. Le directeur de la sécurité informatique. vi. Le directeur des risques. c. L'audit. i. L'audit interne. ii. L'audit externe.	• Toutes les responsabilités portant sur le contrôle des SI ont-elles été attribuées ? • L'allocation des responsabilités est-elle compatible avec les principes de séparation des tâches ? • Les responsabilités en matière de SI sont-elles formalisées ? • Les responsabilités concernant les contrôles des SI ont-elles été communiquées à l'ensemble de l'organisation ? • Les personnes endossant les différents rôles comprennent-elles clairement leurs responsabilités concernant les contrôles des SI ? • Quelles preuves existe-t-il que les titulaires des différents rôles exercent leurs responsabilités ? • L'audit interne emploie-t-il suffisamment de spécialistes informatiques pour examiner les problèmes liés aux contrôles des SI ?

Actions	Questions
4. Identifier le processus d'évaluation des risques. Couvre-t-il : a. L'appétence pour le risque ? b. La tolérance au risque ? c. L'analyse de risques ? d. L'adaptation des contrôles des SI aux risques ?	• Comment sont déterminées l'appétence pour le risque et la tolérance au risque de l'organisation ? • L'appétence pour le risque et la tolérance au risque de l'organisation ont-elles reçu l'aval du Conseil ? • Le niveau d'appétence pour le risque et de tolérance au risque sont-ils clairement compris par tous ceux qui ont des responsabilités en matière de contrôle des SI ? • L'organisation recourt-elle à un processus formel pour l'analyse des risques ? • Ce processus est-il compris par tous ceux qui ont des responsabilités en matière de contrôle des SI ? • Ce processus est-il uniformément utilisé dans toute l'organisation ?
5. Identifier tous les processus de surveillance : a. Imposés par la réglementation. b. Classiques, en interne. c. Autres que l'audit interne.	• Quels processus sont en place pour vérifier que tous les textes de loi, ainsi que les politiques et normes internes, sont bien respectés ? • La direction générale a-t-elle mis en place des processus autres que l'audit interne ?
6. Identifier les mécanismes d'information et de communication : a. Information de contrôle. b. Défaillances de contrôles.	• Quels indicateurs sont fournis au Conseil, à ses comités et à la direction générale concernant la sécurité informatique ? • Quels rapports supplémentaires sont régulièrement fournis au conseil et à la direction générale ? • La direction générale reçoit-elle systématiquement un rapport en cas de défaillance des contrôles des SI ? • Le Conseil et ses comités reçoivent-ils des rapports analogues en cas de défaillance des contrôles des SI ?

A propos du CRIPP

Eléments	Définition
Les dispositions obligatoires. Le respect de ces éléments est exigé et la ligne directrice est élaborée selon le processus requis qui inclut une consultation publique. La conformité aux principes mis en exergue dans les lignes directrices obligatoires est indispensable pour la pratique professionnelle de l'audit interne. Les trois composantes des dispositions obligatoires sont la définition de l'audit interne, le Code de Déontologie et les Normes internationales pour la pratique professionnelle de l'audit interne (Normes).	
Définition	La Définition de l'Audit Interne établit l'objectif fondamental, la nature et le champ d'application de l'audit interne.
Code de déontologie	Le Code de déontologie établit les principes et attentes régissant le comportement des individus et des organisations dans la conduite de l'audit interne. Il décrit les règles minimales de conduite ainsi que des comportements attendus plutôt que des activités spécifiques.
Normes internationales pour la pratique professionnelle de l'audit interne (Normes)	Les Normes sont des principes qui fournissent un cadre pour la réalisation des missions et la promotion de l'audit interne. Elles se composent de Normes de qualification, de Normes de fonctionnement et de Normes de mises en œuvre. Les Normes sont des exigences obligatoires constituées : · de déclarations sur les exigences fondamentales pour la pratique professionnelle de l'audit interne et pour l'évaluation de sa performance. Elles sont internationales et applicables au niveau du service et au niveau individuel. · d'interprétations clarifiant les termes ou les concepts utilisés dans les déclarations. Il est nécessaire de considérer le texte dans sa totalité (c'est-à-dire les déclarations et les interprétations) afin de comprendre et d'appliquer correctement les Normes. Les termes spécifiques utilisés dans les Normes sont explicités dans le Glossaire.

GTAG – A propos du CRIPP

Eléments	Définition
Les dispositions fortement recommandées. La conformité à ces lignes directrices, approuvées par l'IIA, est fortement recommandée. Elles proposent des pratiques pour la mise en œuvre effective de la définition de l'audit interne, du Code de Déontologie de l'IIA et des Normes internationales pour la pratique professionnelle de l'audit interne (Normes). Les trois composantes des dispositions fortement recommandées sont les prises de position, les modalités pratiques d'application (MPA) et les guides pratiques.	
Prises de position	Les Prises de Position aident l'ensemble des parties prenantes, y compris celles qui ne sont pas des professionnels de l'audit interne, à comprendre les principaux enjeux en matière de gouvernance, de risque ou de contrôle. Elles précisent également le rôle et les responsabilités de l'audit interne.
Modalités pratiques d'application (MPA)	Les Modalités Pratiques d'Application fournissent une approche et une méthodologie mais ne précisent pas les processus et les procédures détaillées. Ce sont des lignes directrices qui aident les auditeurs internes dans l'application du Code de déontologie et des Normes ainsi que la promotion des meilleures pratiques. Ces pratiques concernent notamment : • des problématiques internationales, nationales ou spécifiques à certains secteurs d'activité ; • des missions d'audit spécifiques ; • des questions légales ou réglementaires.
Guides pratiques	Les guides pratiques sont des lignes directrices détaillées pour la conduite des activités d'audit interne. Ce sont des processus et des procédures détaillés tels que des outils, des techniques, des programmes, des approches séquentielles (par exemple, des modèles de livrables).

Ce GTAG est un guide pratique du CRIPP.