Lignes directrices complémentaires

GTAG®
Global Technology
Audit Guide

Auditer la gouvernance des systèmes d'information

The Institute of Internal Auditors | Global

À propos des lignes directrices complémentaires

Les lignes directrices complémentaires font partie intégrante du Cadre de référence international des pratiques professionnelles® (CRIPP®) et proposent des recommandations supplémentaires facultatives pour la réalisation des activités d'audit interne. Tout en étayant les *Normes*, elles couvrent des domaines particuliers, ainsi que des problématiques sectorielles, et contiennent des procédures et processus détaillés. Les lignes directrices complémentaires sont homologuées par l'IIA *(the Institute of Internal Auditors)* à l'issue d'un processus formalisé de revue et d'approbation.

Guides pratiques

Les guides pratiques constituent un type de lignes directrices complémentaires qui offrent des approches séquentielles, intégrant des processus, des procédures, des outils et des programmes, ainsi que des exemples de livrables.

Ces guides pratiques sont destinés à aider les auditeurs internes. Il existe aussi des guides pratiques ciblant :

- les établissements financiers
- le secteur public
- les systèmes d'information (GTAG® pour *Global Technology Audit Guide*)

Pour de plus amples informations sur les documents de référence proposés par l'IIA, vous pouvez consulter le site web www.globaliia.org/standards-guidance

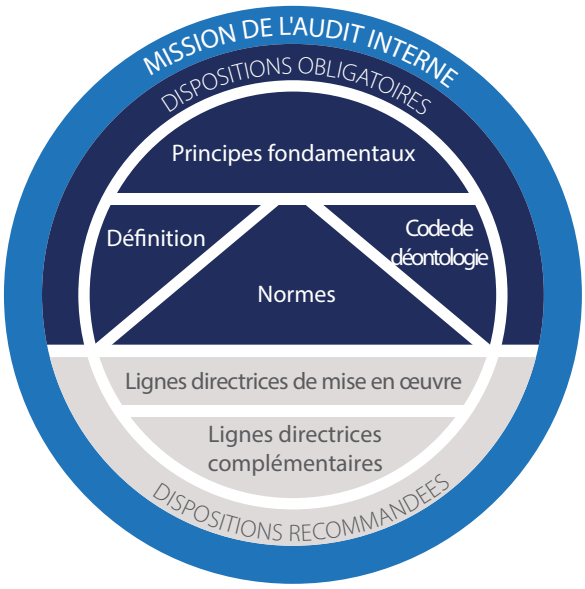


Table des matières

Synthèse 4

Introduction 5

Aperçu de la gouvernance des systèmes d'information 6

- Enjeux métiers 8
- Les principaux risques 10
- Les composantes de la gouvernance des systèmes d'information 10
- Le rôle de l'audit interne dans la gouvernance des systèmes d'information 12
  - La compétence 13

La planification de la mission 15

- 1. Comprendre le contexte et l'objectif de la mission 15
- 2. Collecter les informations 17
  - 2.1 Obtenir et documenter l'information 17
  - 2.2 S'entretenir avec les parties prenantes concernées 18
- 3. Réaliser une évaluation préliminaire des risques 19
- 4. Définir les objectifs de la mission 20
  - 4.1 Les objectifs de la mission de conseil 21
- 5. Établir le périmètre d'intervention de la mission 22
- 6. Allocation des ressources 23
- 7. Documenter le plan 23

La communication des résultats de la mission 24

Annexe A. Normes et lignes directrices de l'IIA applicables 25

Annexe B. Glossaire 26

Annexe C. Questionnaire de contrôle interne relatif à la gouvernance des SI 28

Annexe D. Matrice des risques et des contrôles relative à la gouvernance des SI 31

Annexe E. Ressources supplémentaires 39

Remerciements 40

Synthèse

Adopter une approche stratégique pour la mise en œuvre de la gouvernance des systèmes d'information (SI) aide les organisations à répondre aux avancées technologiques rapides, à la multiplication des prestations liées aux SI et à la grande dépendance envers ces systèmes pour l'atteinte des objectifs de l'organisation. Une gouvernance performante des SI contribue à l'efficience et à l'efficacité des contrôles et permet à l'organisation de tirer des bénéfices financiers et extra-financiers de ces investissements dans les SI. Souvent, des contrôles mal conçus ou défaillants trouvent leur cause première dans une gouvernance médiocre ou inefficace des SI.

> L'alignement du SI et des objectifs de l'organisation a plus à voir avec la gouvernance qu'avec la technologie. La gouvernance veille à ce que les alternatives soient évaluées, que l'exécution soit correctement dirigée et que les risques et la performance soient surveillés.

La gouvernance des SI est directement liée au pilotage des actifs et des risques associés aux SI et de ce fait, elle est sous la responsabilité partagée de la direction générale[1] et du Conseil. La direction générale gère les activités courantes pour être tactiquement en phase avec les orientations stratégiques du Conseil et aboutir à un usage efficace, efficient et acceptable des ressources des systèmes d'information. Les principaux résultats d'une gouvernance des SI efficace sont les suivants :

- les stratégies SI sont alignées sur les objectifs de l'organisation;
- les risques sont correctement identifiés et gérés;
- les investissements en matière de SI sont optimisés pour créer de la valeur pour l'organisation;
- la performance des SI est définie, mesurée et communiquée au moyen d'indicateurs significatifs;
- les ressources liées aux systèmes d'information sont efficacement gérées.

Une gouvernance inexistante ou médiocre des SI peut avoir des impacts négatifs importants sur une organisation, aussi bien au niveau financier que de la réputation. Le retour à la normale après de telles conséquences exige du temps, de l'énergie et de l'argent. Dans de nombreuses organisations, la direction générale est déconnectée des sujets SI à cause d'une vieille idée selon laquelle les SI ne servent qu'à fournir des prestations informatiques quotidiennes. Dans la réalité, les SI sont essentiels au développement de l'avantage concurrentiel et à l'atteinte des buts et des objectifs stratégiques de l'organisation.

La fonction d'audit interne jouit d'un positionnement singulier et de ressources humaines exceptionnelles pour vérifier si la gouvernance des SI de l'organisation soutient la stratégie et les objectifs (Norme de mise en œuvre 2210.A2).

Cette deuxième édition du GTAG « *Auditing IT Governance* » tient compte du Cadre de référence international des pratiques professionnelles actualisé en 2017 et donne davantage de conseils pratiques aux auditeurs internes.

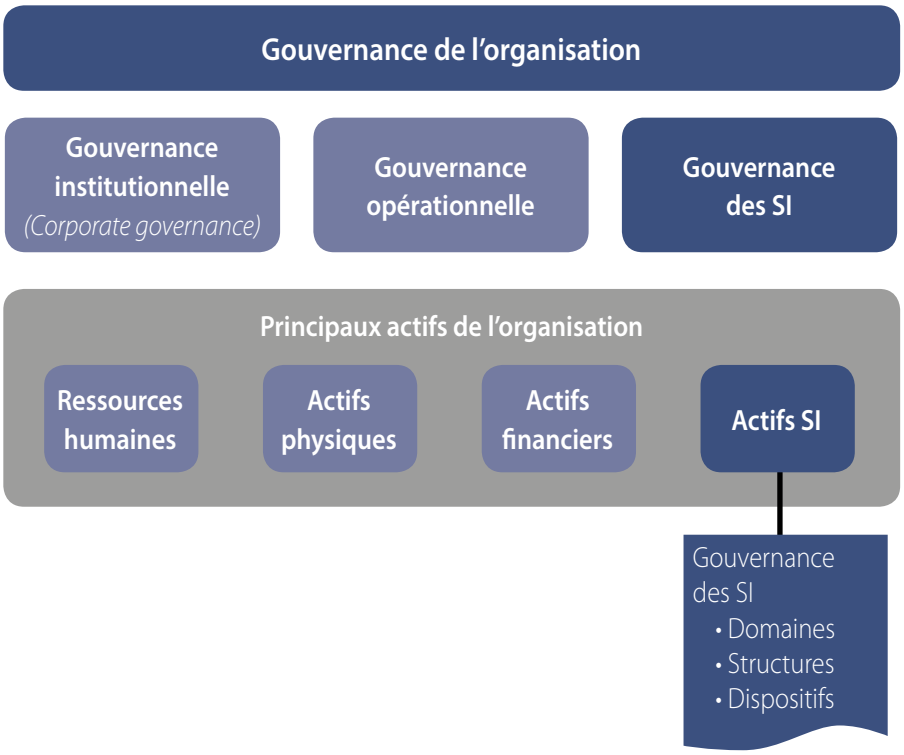
[1] La direction générale inclut généralement le directeur général, le directeur financier, le directeur des opérations, et le directeur du marketing.

Introduction

La gouvernance de l'organisation, qui constitue le niveau le plus élevé de gouvernance, est défini dans les *Normes internationales pour la pratique professionnelle de l'audit interne* comme étant : « Le dispositif comprenant les processus et les structures mis en place par le Conseil afin d'informer, de diriger, de gérer et de piloter les activités de l'organisation en vue de réaliser ses objectifs ».

La gouvernance des SI est un domaine de la gouvernance de l'organisation. Elle comprend la direction, les structures organisationnelles et les processus qui garantissent que les systèmes d'information soutiennent la stratégie et les objectifs de l'organisation. La gouvernance des SI soutient les exigences réglementaires, légales, environnementales et opérationnelles de l'organisation pour lui permettre d'atteindre ses plans et ses ambitions stratégiques. D'autres domaines de la gouvernance de l'organisation comprennent la gouvernance liée aux processus de conformité ou encore celle qui concerne les processus de performance. La **figure n°1** montre le lien entre la gouvernance de l'organisation et la gouvernance des SI.

Figure 1 : Lien entre la gouvernance de l'organisation et la gouvernance des SI



Adapté de : L'Institut de la Gouvernance des Systèmes d'Information, Place de la gouvernance du système d'information dans la gouvernance générale de l'entreprise, 2005

L'objectif de ce guide est d'accompagner les auditeurs internes dans la prestation de services d'assurance en relation avec la gouvernance des SI. Le guide fournit une description détaillée des processus, des pratiques et de la terminologie de la gouvernance des SI afin d'aider les auditeurs internes à comprendre le concept de gouvernance et les caractéristiques des processus de bonne gouvernance.

Cette édition propose des outils et des techniques aidant les auditeurs internes à développer un programme de travail et à réaliser des missions en lien avec la gouvernance des SI.

Aperçu de la gouvernance des systèmes d'information

La mise en œuvre de la gouvernance des SI est un élément incontournable de la stratégie puisqu'elle est fondamentalement impactée par les objectifs visant à s'assurer que les SI apportent effectivement de la valeur aux métiers. Un cadre de référence type en matière de gouvernance des SI s'articule autour de cinq aspects majeurs :

- Alignement stratégique – La gouvernance des SI donne une orientation stratégique aux systèmes d'information et facilite l'alignement SI – métiers au niveau des services, des projets, des objectifs opérationnels, de l'actualisation de la stratégie des SI et de l'articulation des objectifs opérationnels avec les initiatives en matière de SI.
- Management des risques – La gouvernance des SI contribue à déterminer quels processus sont en place pour assurer que les risques ont été correctement traités. En outre, elle peut donner l'assurance que le management des risques de l'entreprise prend en compte les risques liés aux investissements SI, définit les responsabilités en la matière, comprend une méthodologie d'analyse des risques commune et des stratégies pour traiter les risques. Elle vise aussi à établir une surveillance continue des menaces, de l'occurrence et de l'impact de manière holistique.
- Création de valeur – La gouvernance des SI facilite une coordination SI – métiers conçue pour optimiser l'apport des SI dans la création de valeur métiers. Les directions métiers sont alors en mesure de piloter la création de valeur par les SI et de mesurer le retour sur investissement (ROI), l'exécution du plan tactique des SI et les bénéfices visibles pour chaque niveau de l'organisation. Par exemple, le temps de fonctionnement du système (stratégie de l'infrastructure), le degré d'automatisation dans la stratégie de développement du logiciel (SDLC- *System Development Life Cycle*), la productivité (stratégie opérationnelle), et l'impact financier (stratégie financière des SI).
- Mesure de la performance – La gouvernance des SI fournit les mécanismes de vérification du respect de la stratégie (ex : atteinte des objectifs stratégiques en matière de SI), de mesure de la performance des systèmes d'information et de leur contribution au résultat net (ex : les fonctionnalités métiers promises sont-elles effectives ?). Il existe d'autres moyens tels que le suivi en continu et le reporting, les procédures de suivi, l'analyse causale et la gestion des problèmes, l'étude comparative au regard des pratiques du secteur ou des normes et cadres de référence éprouvés.
- Gestion des ressources – La gouvernance des SI définit la stratégie globale de gestion et d'utilisation des ressources. Elle contribue à s'assurer que les capacités et l'infrastructure des SI sont adéquates pour soutenir les besoins actuels et futurs des métiers, les stratégies de gestion des ressources, les pratiques de gestion des ressources humaines, les manuels d'utilisateur, la séparation des tâches, le suivi du temps passé, la gestion du cycle de vie de l'infrastructure, les accords de niveau de service *(Service Level Agreement* - SLA) et des politiques d'utilisation acceptables.

La gouvernance des SI peut aider les organisations à relever notamment les défis suivants :

- la complexité croissante des environnements SI ;
- une dépendance croissante de la prise de décision opérationnelle vis-à-vis des données ;
- la multiplication des appareils mobiles ;
- le besoin d'échanger des informations avec les clients, les prestataires de services et les partenaires ;
- le risque croissant de cyber-attaques ;
- un accroissement de lois et réglementations sur la protection des données.

Dans le cadre conceptuel de gouvernance des SI, la direction générale et le Conseil sont responsables de la définition :

- des objectifs liés aux SI de l'organisation en concordance avec la stratégie globale des métiers ;
- de la stratégie SI pour atteindre les objectifs métiers ;
- des politiques de gouvernance ;
- des structures organisationnelles ;
- des processus de management des risques associés.

La direction des systèmes d'information (DSI) est responsable des activités courantes : planification, exécution et supervision de l'usage des ressources SI qui soutiennent la stratégie et les politiques établies par le Conseil.

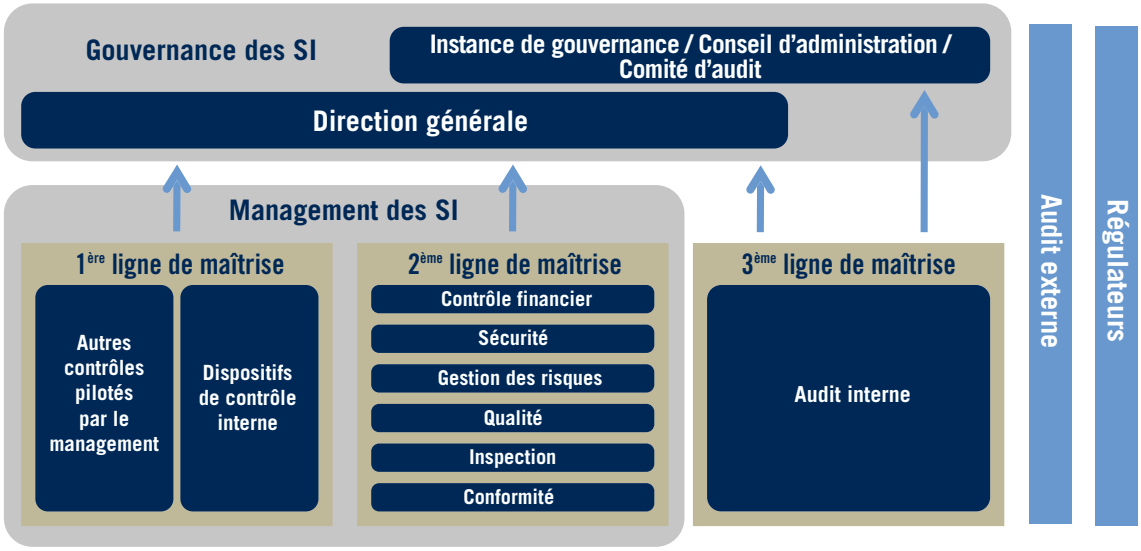
Le rôle de l'audit interne dans la gouvernance des SI est devenu de plus en plus important à la suite des crises financières internationales et des failles majeures dans la sécurité de l'information. Selon les résultats du CBOK® publiés par l'IIA dans un rapport intitulé *Promouvoir et soutenir l'efficacité de la gouvernance de l'organisation,* l'audit interne est bien positionné pour promouvoir et soutenir la gouvernance de l'organisation, et ainsi aider l'organisation à trouver le juste équilibre entre création de valeur et préservation de valeur.

L'audit interne a, en tant que troisième ligne de maîtrise, notamment la responsabilité d'évaluer et de formuler des recommandations en vue d'améliorer les processus de gouvernance de l'organisation (Norme 2110 – Gouvernance) pour contribuer à la prévention des défaillances de gouvernance et à l'amélioration de la performance stratégique.

En effet, selon le modèle des trois lignes de maîtrise, le management opérationnel (DSI inclus) représente la première ligne de maîtrise. Il est responsable de la mise en œuvre et du maintien des processus et des contrôles liés au management des risques. Les fonctions de conformité et de gestion des risques représentent la deuxième ligne de maîtrise et sont responsables du suivi des risques dans toute l'organisation. L'audit interne représente la troisième ligne de maîtrise et doit donner une assurance indépendante sur le bon fonctionnement du management des risques et des dispositifs de contrôle et conseiller la direction générale et le Conseil lorsque des problèmes sont identifiés.

La **figure n°2** montre les responsabilités de gouvernance des systèmes d'information selon le modèle des trois lignes de maîtrise.

Figure 2 : Les trois lignes de maîtrise dans le cadre de la gouvernance des systèmes d'information



Source : Prise de position de l'IIA : Modèle des trois lignes de maîtrise pour une gestion des risques et un contrôle efficaces (Altamonte Springs, Floride, États-Unis : Institute of Internal Auditors, 2013). Schéma adapté à partir des lignes directrices ECIIA/FERMA sur la 8e directive de l'UE relative au droit des sociétés, article 41.

De nombreux cadres de référence sur la gouvernance des SI reconnus à l'échelle internationale pourront compléter cette note explicative. Des cadres de référence comme ITIL®, COBIT®, ISO/IEC 38500, King III, et King IV couvrent plus en détails les processus et dispositifs nécessaires au développement, à la mise en œuvre, à l'évaluation et à l'amélioration d'un programme de gouvernance des systèmes d'information. Ce guide se concentre sur les processus et les dispositifs que l'audit interne peut utiliser pour vérifier que la gouvernance des systèmes d'information de l'organisation soutient la stratégie et les objectifs de l'organisation, conformément à la Norme de mise en œuvre 2110.A2.

Enjeux métiers

L'information et les composantes technologiques font partie des actifs les plus importants d'une organisation. Une gouvernance inappropriée de l'information stockée, traitée ou produite par les systèmes d'information peut avoir un impact négatif significatif sur une organisation, que ce soit sous la forme d'amendes et de sanctions, ou d'une réputation entachée dont la réhabilitation peut prendre du temps, de l'énergie et de l'argent. En bref, la gouvernance des SI peut influencer et avoir des effets sur toute l'organisation et pas uniquement sur la DSI.

Cette dépendance accrue vis-à-vis des systèmes et de l'information signifie que les organisations ont tout intérêt à investir plus de ressources pour améliorer et maintenir leurs environnements SI. Ces derniers sont censés faciliter le management des risques, l'amélioration des opérations et la création de valeur en fournissant des services permettant d'atteindre les objectifs financiers et extra-financiers de l'organisation.

L'objectif premier de la gouvernance des systèmes d'information est l'alignement des priorités de l'organisation et des objectifs en matière de SI pour s'assurer que les efforts dans ce domaine se concentrent sur les processus ou projets qui soutiennent les objectifs stratégiques. Un bon alignement entre l'organisation et les systèmes d'information se produit lorsque la direction générale et le Conseil comprennent la valeur stratégique des systèmes d'information, et reconnaissent leur contribution au résultat net.

Un bon alignement entre l'organisation et les systèmes d'information signifie que :

- la direction générale et le Conseil comprennent le potentiel et les limites des systèmes d'information ;
- l'équipe de direction de la fonction SI comprend les objectifs de l'organisation et les besoins qui en découlent ;
- cette compréhension est déclinée et surveillée dans toute l'organisation au moyen d'une bonne gouvernance et d'un devoir de rendre compte.

Un cadre de référence solide de gouvernance des SI apporte toute une série de bénéfices :

- un avantage concurrentiel ;
- un accès plus rapide au marché ;
- une sécurité de l'information et une conformité efficaces ;
- une automatisation des processus et de l'innovation ;
- une prise de décision plus avisée et éclairée ;
- une meilleure compréhension des causes premières des problèmes pour une amélioration continue des processus.

Les activités reprises dans le périmètre de la gouvernance des systèmes d'information incluent[2] :

- un alignement des investissements et des priorités en matière de SI avec les objectifs métiers ;
- une gestion, une évaluation, une priorisation, un financement ainsi qu'une mesure et une surveillance plus cohérents et reproductibles des demandes de prestations SI, des travaux et des livrables qui en résultent pour une optimisation du service rendu aux métiers ;
- une utilisation responsable des ressources et des actifs ;
- un devoir de rendre compte et une autorité de décision clairement établis – des rôles et pouvoirs clairement définis ;
- une assurance que les systèmes d'information correspondent aux plans, budgets et engagements ;
- une gestion proactive des risques, menaces, changements et imprévus ;
- une amélioration de la performance, de la conformité, de la maturité, du développement des collaborateurs et de la sous-traitance ;
- une promotion de l'innovation au niveau des systèmes d'information et dans l'ensemble de l'organisation.

[2] *Selig, Grad J., Implementing IT Governance: A Practical Guide to Global Sect Practices in IT Management, Van Haren Publishing, Zaltbommel, mars 2008.*

Les principaux risques

Tout comme les impacts positifs de la gouvernance des SI permettent à l'organisation d'atteindre ses objectifs financiers et extra-financiers, d'améliorer les opérations, et de contrôler les risques ; les impacts négatifs peuvent être néfastes pour toute l'organisation.

Mettre l'accent sur les aspects financiers ou techniques des SI au détriment du contexte organisationnel où les SI sont des leviers pour les métiers, peut conduire à des résultats négatifs, un faible retour sur investissement en matière de SI ou une incapacité à démontrer les bénéfices générés par les investissements en SI.

D'autres exemples d'impacts négatifs :

- des pertes financières dues à une perturbation des activités ;
- des coûts plus élevés pour le fonctionnement des opérations ;
- des attentes de nouveaux clients non satisfaites et des clients mécontents ;
- les principaux processus de l'activité subissent l'incidence négative de mauvaises prestations SI ;
- des risques et des menaces non identifiés exposent toute l'organisation à des violations de la sécurité ;
- des sanctions résultant de manquements aux exigences réglementaires.

Les composantes de la gouvernance des systèmes d'information

La mise en œuvre et le maintien d'un programme de gouvernance des SI s'articulent autour de composantes pouvant aider la direction générale et le Conseil à diriger, surveiller et mesurer la performance des systèmes d'information. Comme le montre la **figure n° 3,** les composantes clés d'une gouvernance des SI efficace ont été regroupées en trois catégories :

- *Les processus* – Incluent tous les processus SI mis en œuvre pour fournir des services à l'organisation (ex: gestion du changement, gestion de la sécurité de l'information, développement de logiciel et gestion de projet).
- *Les structures organisationnelles* – Incluent les rôles et rattachements nécessaires pour que les SI répondent aux besoins de l'organisation tout en respectant les exigences au moyen d'évaluation et de priorisation formelles **(figure n° 4).**
- *Les dispositifs* – Incluent les normes, les politiques et les cadres de référence mis en œuvre pour diriger, surveiller et mesurer la performance des systèmes d'information. Le cadre de référence de la gouvernance des SI devrait déterminer quels processus doivent être en place pour s'assurer que les risques ont été identifiés, évalués correctement et traités ou acceptés en accord avec l'appétence et la tolérance au risque de l'organisation.

Figure 3 : Les composantes de la gouvernance des systèmes d'information

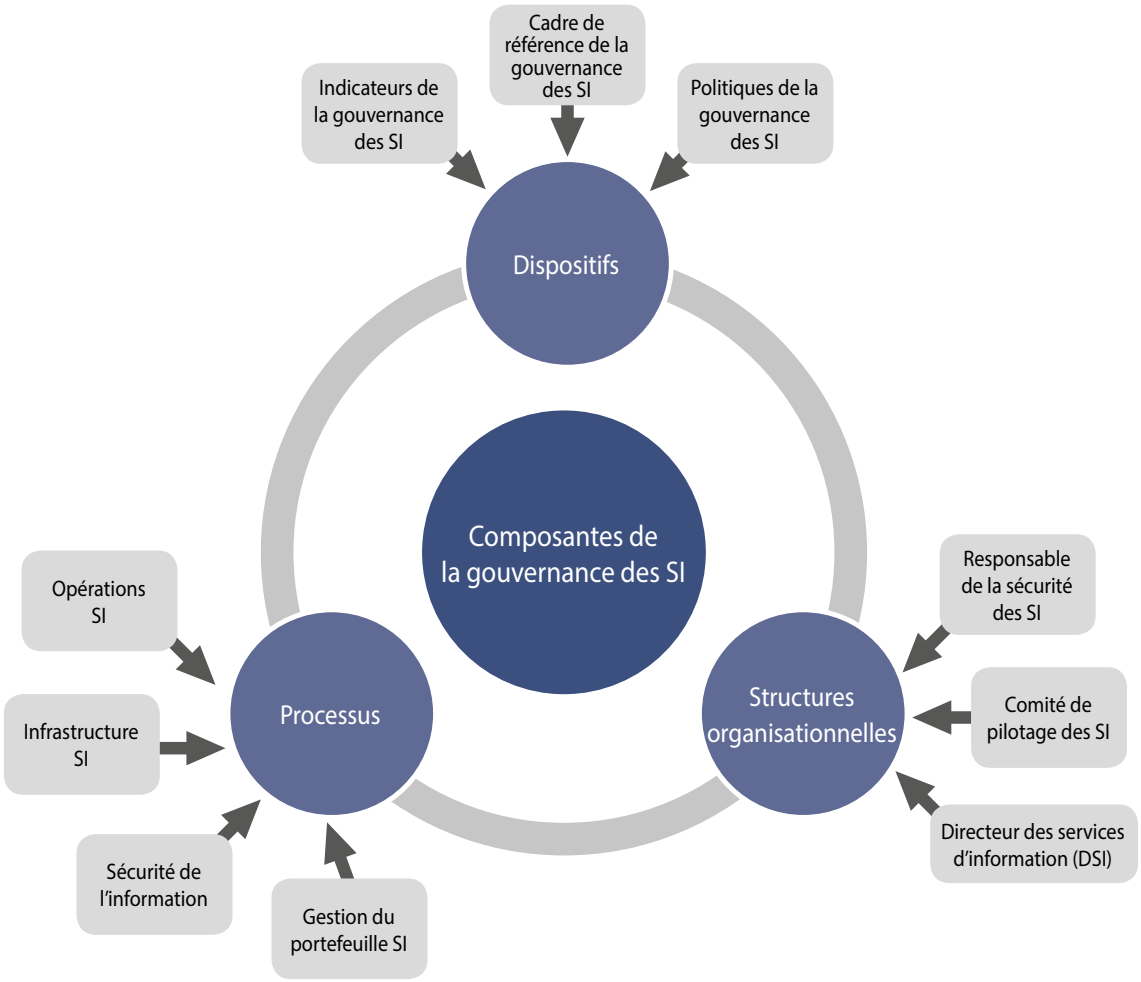


Figure 4 : Exemples de structures organisationnelles

Organe de gouvernance	Membres	Périmètre
Instance de gouvernance des SI	Directeur général, directeur financier, DSI, responsable de l'audit interne*	Stratégie et plans d'investissement métiers et SI
Comité de pilotage des SI	Direction générale, propriétaires d'unité opérationnelle	Alignement stratégique des SI
Instance chargée du portefeuille SI	Chefs de programme SI, chefs de programme/projet métiers, chefs de projet SI	Indicateurs, surveillance et reporting de projet SI
Instance chargée de l'architecture SI	DSI, responsable de la sécurité des SI, directeur des opérations, manager de l'infrastructure SI	Conception de l'architecture SI
Le comité des technologies	Le DSI, le responsable des infrastructures informatiques, les propriétaires d'unité opérationnelle	Évaluation des opportunités technologiques
Le comité de la cybersécurité et de la protection des données	Le DSI, le directeur des infrastructures informatiques, le responsable de la sécurité des SI, le responsable du management des risques, le directeur financier, le directeur des opérations, le responsable de l'audit interne et les propriétaires d'unité opérationnelle	Évaluation des risques et de la stratégie de l'organisation afin de protéger ses actifs informationnels

* Note : Le responsable de l'audit interne siège dans l'instance de gouvernance en tant que conseiller en matière de risques et de contrôles. Il ne vote pas les décisions prises.

Le rôle de l'audit interne dans la gouvernance des systèmes d'information

La gouvernance des SI est une responsabilité managériale. L'audit interne devra rester indépendant mais cela lui confère une position idéale pour influencer et recommander le changement.

Il est impératif que les missions d'audit de la gouvernance des SI soient réparties en activités d'assurance et en activités de conseil selon la robustesse du système de gouvernance des SI en place. L'indépendance ne devrait pas faire obstacle aux prestations de conseil tant que la direction générale assume pleinement la responsabilité et le devoir de rendre compte pour la mise en œuvre et le fonctionnement des dispositifs de contrôle.

Tout type d'audit peut permettre d'évaluer si les responsables métiers suivent les politiques et protègent suffisamment les actifs en collaborant avec les responsables des systèmes d'information pour identifier les risques et les contrôles.

Les processus de gouvernance sont pris en considération lors de l'évaluation des risques et du développement du plan d'audit réalisés par la fonction d'audit interne. Le responsable de l'audit interne identifie généralement les processus de gouvernance des risques les plus importants, traités lors de missions d'assurance et de conseil décrits dans le plan d'audit final. En outre, le Guide de mise en œuvre de la Norme 2110 précise que la fonction d'audit interne a la responsabilité de produire une évaluation et des recommandations appropriées destinées à améliorer les processus de gouvernance de l'organisation pour :

- les prises de décisions stratégiques et opérationnelles ;
- la surveillance des processus de management des risques et de contrôle ;
- la promotion des règles d'éthique et des valeurs appropriées au sein de l'organisation ;
- une gestion efficace des performances de l'organisation, assortie d'une obligation de rendre compte ;
- la communication aux services concernés des informations relatives aux risques et aux contrôles ;
- la coordination des activités et la communication des informations entre le Conseil, les auditeurs externes, les auditeurs internes, les autres prestataires d'assurance, et le management.

Facteurs de renforcement de la gouvernance des systèmes d'information :

- Une responsabilisation et un devoir de rendre compte des SI clairement établis.
- Le rattachement du DSI à la direction générale.
- La contribution des SI à l'innovation est reconnue.
- La performance des SI est surveillée et mesurée.

Les missions d'audit interne de la gouvernance des SI devraient se concentrer sur la mise en œuvre des pratiques de gouvernance de l'organisation. Celles-ci comprennent des politiques, des rôles et des responsabilités clairement définis, un alignement des appétences pour le risque, une communication efficace, l'exemplarité au plus haut niveau, la gestion de la valeur des SI et un devoir de rendre compte explicite. Les évaluations de l'audit interne incluent les activités suivantes :

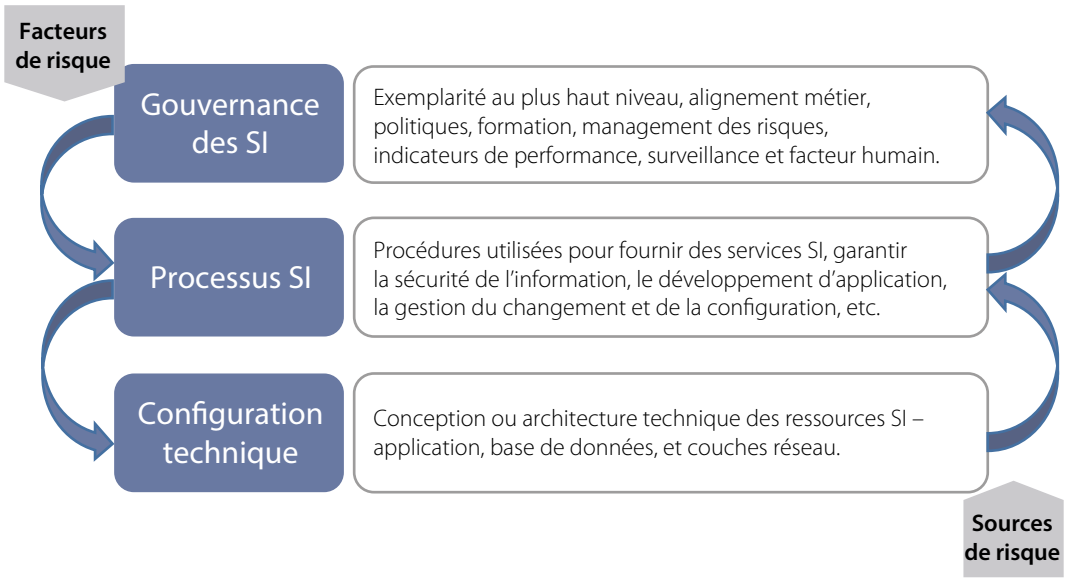
- évaluer le niveau de cohérence des activités et des normes de gouvernance avec l'appétence pour le risque de l'organisation telle qu'elle a été comprise par la fonction d'audit interne ;
- réaliser des missions de conseil comme le prévoit la charte d'audit et l'autorise le Conseil ;
- développer un dialogue permanent avec l'instance de gouvernance des SI afin de s'assurer que les changements majeurs dans l'organisation et au niveau des risques sont traités en temps utile.

Lors de l'évaluation de la gouvernance, l'audit interne doit aller au-delà de la simple identification des problèmes. Les auditeurs internes devraient identifier les causes premières et faire des recommandations constructives dès que des faiblesses au niveau des contrôles des SI sont identifiées, par exemple, une configuration du pare-feu défaillante. Dans ce cas précis, une évaluation de la cause première peut inclure un contrôle en plusieurs étapes afin d'identifier la source du problème.

La figure n°5 montre un cadre d'analyse causale avec un contrôle en trois étapes pouvant être utilisé pour l'évaluation des faiblesses des systèmes d'information. Elle commence par une analyse technique, suivie d'une analyse des processus et d'une recherche de dysfonctionnements à l'origine de la défaillance de la configuration du pare-feu (ex : manque de surveillance ou de pilotage, ou séparation des tâches inadaptée).

Après l'analyse des processus, il s'agit de passer à l'analyse de la gouvernance des SI et de vérifier si l'organisation dispose de pratiques de gouvernance des SI efficaces telles que l'analyse des risques, le développement de politiques, la maintenance et une formation à propos des pare-feu.

Figure 5 : Risques SI – cadre d'analyse causale



La fonction d'audit interne crée de la valeur lorsqu'elle identifie les causes premières et assure la conception de plans d'actions constructifs en collaboration avec le management pour résoudre le problème.

La compétence

Comme repris dans la Norme de mise en œuvre 2130. A1, l'évaluation de la gouvernance peut impliquer des missions d'assurance et/ou de conseil afin d'évaluer l'adéquation et l'efficacité du dispositif de contrôle choisi pour faire face aux risques relatifs à la gouvernance, aux opérations et systèmes d'information de l'organisation et assurer :

Alors que la gouvernance des SI pourrait sembler nécessiter une expérience approfondie des systèmes d'information, les aspects stratégiques de la gouvernance des SI peuvent s'inscrire dans toute mission d'audit interne portant sur les métiers.

- l'atteinte des objectifs stratégiques de l'organisation ;
- la fiabilité et l'intégrité des informations financières et opérationnelles ;
- l'efficacité et l'efficience des opérations et des programmes ;
- la protection des actifs ;
- la conformité aux lois, règlements, politiques, procédures et contrats.

La planification de la mission

Selon la Norme 2200 – Planification de la mission, les auditeurs internes doivent concevoir et documenter un plan pour chaque mission. Ce plan de mission précise les objectifs, le périmètre d'intervention, le calendrier de la mission, ainsi que les ressources allouées. Ce plan doit prendre en considération la stratégie, les objectifs et les risques de l'organisation pertinents au regard de la mission. Cette section a pour vocation d'aider l'auditeur interne à définir les domaines clés à inclure dans la mission de gouvernance des SI, les types de documents à solliciter, les questions à inclure lors des entretiens et les éléments probants à obtenir. Les exemples fournis ne sont pas exhaustifs.

La planification de la mission inclut généralement les étapes suivantes :

- Comprendre le contexte et l'objectif de la mission.
- Rassembler les informations afin de comprendre le domaine ou le processus audité.
- Réaliser une évaluation préliminaire des risques liés au domaine ou au processus audité.
- Définir les objectifs de la mission.
- Établir le périmètre d'intervention de la mission.
- Affecter les ressources.
- Documenter le plan.

Pour des informations détaillées sur la manière de planifier et d'orienter une mission d'audit, référez-vous au Guide pratique de l'IIA « Planification de la mission : Définir les objectifs et le périmètre d'intervention ».

Lors de la planification de la mission, la fonction d'audit interne doit avant tout déterminer si l'organisation dispose d'une structure de gouvernance unifiée et cohérente, y compris des politiques, procédures et outils pour gérer l'environnement et contrôler les risques liés aux SI en continu.

Il peut être difficile d'évaluer tout le programme de gouvernance des SI. Aussi, le périmètre de la mission d'audit peut-il être défini selon des critères répondant à un objectif spécifique. Par exemple, le périmètre peut être défini en fonction des unités organisationnelles, des sites, de l'objectif stratégique de l'organisation ou selon tout autre critère pertinent pour l'organisation.

1. Comprendre le contexte et l'objectif de la mission

Le responsable de l'audit interne et les auditeurs internes cherchent en premier lieu à comprendre le concept de gouvernance et les caractéristiques des processus classiques de gouvernance. Ils sont également tenus d'examiner la définition du terme « gouvernance » dans le glossaire des *Normes internationales pour la pratique professionnelle de l'audit interne,* et de se familiariser avec les référentiels et les modèles, mondialement reconnus en matière de gouvernance (comme les cadres de référence du *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) ou les normes 31000 et 38500 de l'Organisation internationale de normalisation (ISO)).

Les référentiels, modèles et règles de gouvernance varient selon les organisations et les juridictions. La manière dont une organisation conçoit et met en œuvre les principes d'une gouvernance efficace dépend aussi de facteurs comme sa taille, sa complexité, son cycle de vie, sa maturité, la structure de son actionnariat, et les obligations légales auxquelles elle est soumise.

L'approche de l'audit interne en matière d'évaluation de la gouvernance et de recommandations variera en fonction du référentiel ou du modèle utilisé par l'organisation.

L'audit interne doit avant tout demander quel cadre de référence l'organisation utilise pour mettre en place la gouvernance des systèmes d'information. Si l'organisation ne dispose pas de cadre de référence, l'audit interne peut proposer de réaliser une mission de conseil pour aider la direction générale à dresser une cartographie des contrôles et pratiques en place selon un cadre de référence convenu.

Le responsable de l'audit interne se demande ensuite si le plan d'audit interne recouvre les processus de gouvernance de l'organisation et les risques qui leur sont associés. La gouvernance n'est pas constituée d'une série de processus et de structures indépendants. En effet, les processus de gouvernance, de management des risques et de contrôle sont liés. Par exemple, dans le cadre d'une gouvernance efficace, les risques seront pris en compte lors de la définition de la stratégie. De même, le management des risques s'appuie sur une gouvernance efficace (exemplarité au plus haut niveau, appétence pour le risque, seuil de tolérance au risque et culture du risque ainsi que la surveillance du management des risques). Dans le même esprit, une gouvernance efficace s'appuie sur des dispositifs de contrôle interne et sur une communication de leur efficacité au Conseil.

Selon le Guide de mise en œuvre de la Norme 2110 – Gouvernance, « le responsable de l'audit interne peut passer en revue la charte du Conseil et de ses comités spécialisés, ainsi que les ordres du jour et les procès-verbaux de réunions, pour avoir une idée du rôle joué par le Conseil dans la gouvernance de l'organisation, surtout en ce qui concerne les prises de décisions stratégiques et opérationnelles. Le responsable de l'audit interne peut également s'entretenir avec d'autres acteurs clés de la gouvernance (par exemple le Président du Conseil, le principal dirigeant élu ou nommé d'une entité du secteur public, le responsable de la déontologie, le responsable des ressources humaines, l'auditeur externe, le responsable de la conformité, le responsable du management des risques, etc.) pour mieux comprendre les processus spécifiques à l'organisation, et les prestations d'assurance déjà en place. Si l'organisation est régulée, le responsable de l'audit interne pourra examiner les éventuels problèmes de gouvernance soulevés par le ou les régulateurs.

Il est fondamental de bien comprendre la gouvernance pour pouvoir discuter avec le Conseil et la direction générale sur ce qui constitue la gouvernance et les attentes à cet égard. Ainsi, une approche et un plan d'audit interne appropriés pourront être mis en œuvre ».

Une bonne gouvernance des SI en un clin d'œil

- Les structures organisationnelles et de gouvernance en place donnent une bonne indication de l'efficacité du soutien et de la contribution fournis par les systèmes d'information pour atteindre les objectifs stratégiques de l'organisation.
- Il est important de déterminer l'efficacité de l'exemplarité au plus haut niveau, la manière dont elle est communiquée à tous les niveaux de l'organisation et comment ce message entre en résonance avec les systèmes d'information.
- Les indicateurs de prestation de services, y compris la gestion financière, sont des éléments importants de contrôle et de surveillance de la mesure des coûts/avantages.
- La gestion stratégique de la performance est une composante essentielle d'une gouvernance des SI efficace, permettant de piloter les besoins de l'organisation et les services SI par des dispositifs éprouvés.

2. Collecter les informations

Il est important que les auditeurs internes documentent les informations collectées alors qu'ils élaborent le plan, conformément à la Norme 2200 – Planification de la mission. Il est intéressant de noter que ce processus n'est pas toujours constitué d'un nombre défini d'étapes qui se suivent dans un ordre séquentiel. Il s'agit plutôt d'un processus continu à mettre à jour tout au long de la planification de la mission à mesure que de nouvelles informations sont obtenues lors de la prise de connaissance des évaluations précédentes (ex : évaluations des risques et rapports fournis par des prestataires de services d'assurance et de conseil), de la compréhension et de la cartographie de flux de processus et de contrôle ou d'entretiens avec les parties prenantes correspondantes.

Le Guide de mise en œuvre de la Norme 2110 indique que, en général, ce n'est pas une mission unique d'audit de la gouvernance qui est effectuée. L'audit interne évalue plutôt les processus de gouvernance en se fondant sur les informations obtenues, au fil du temps, lors de diverses missions d'audit.

Si une évaluation globale de la gouvernance est appropriée, elle devra prendre en compte :

- les résultats des missions d'audit des processus de gouvernance spécifiques mentionnés ci-dessus ;
- les problèmes de gouvernance relevés dans le cadre de missions qui n'étaient pas spécialement centrées sur la gouvernance, comme les missions concernant :
    - la planification stratégique,
    - l'efficacité et l'efficience opérationnelle,
    - le contrôle interne relatif à la communication financière,
    - les risques liés aux systèmes d'information, à la fraude, et à d'autres domaines,
    - la conformité aux lois et règlements applicables.
- les résultats des évaluations des risques ;
- les résultats des évaluations par le management (par exemple, les inspections de conformité, audits qualité, auto-évaluations des contrôles) ;
- le travail de prestataires d'assurance externes (par exemple, des enquêteurs judiciaires, des contrôleurs des finances publiques, des cabinets d'audit externe) et des régulateurs ;
- les travaux de prestataires d'assurance internes ou de fonctions de la seconde ligne de maîtrise (par exemple santé et sécurité, conformité, qualité) ;
- d'autres informations sur les questions de gouvernance, comme des incidents indésirables indiquant des opportunités d'amélioration des processus de gouvernance.

2.1 Obtenir et documenter l'information

Obtenir une compréhension détaillée de l'organisation et de la gouvernance des SI permet aux auditeurs internes de procéder à une évaluation préliminaire des risques pertinents, comme l'exige la Norme 2210.A1. Les sources d'information incluent la documentation et les entretiens avec les parties prenantes.

À l'issue de cette étape, le plan de mission devrait au minimum contenir :

- les objectifs du domaine audité ;
- les approches utilisées pour atteindre lesdits objectifs ;
- les risques pouvant empêcher l'atteinte des objectifs ;

- les processus et contrôles clés ;
- les SI et autres systèmes pertinents pour le domaine ou processus audité ;
- les sources et la fiabilité des données entrantes et sortantes du domaine ou du processus audité.

Exemples de documentation que l'auditeur interne peut solliciter pour planifier la mission d'audit interne de la gouvernance des SI :

- les rapports d'audit antérieurs ;
- les plans stratégiques (mission et vision de l'organisation) ;
- le cadre de référence de la gouvernance de l'organisation ;
- le cadre de référence de la gouvernance des SI ;
- la politique en matière de sécurité de l'information ;
- les politiques en matière d'architecture SI ;
- les organigrammes ;
- la stratégie et les objectifs de l'organisation ;
- les rapports relatifs au management des risques de l'entreprise (ERM - *Entreprise Risk Management*) ;
- les rapports concernant la performance des SI ;
- les procès-verbaux de réunions sur la gouvernance ;
- les procès-verbaux de réunions du Conseil et du comité ;
- les rapports du management ;
- les approbations des exceptions et la documentation y afférente.

L'Annexe C propose un questionnaire de contrôle interne permettant aux auditeurs internes d'acquérir une compréhension approfondie de l'environnement existant en matière de gouvernance des SI et de définir au mieux le périmètre, le plan et la réalisation de la mission d'audit.

2.2 S'entretenir avec les parties prenantes concernées

Les entretiens avec les parties prenantes constituent une étape essentielle pour la compréhension par les auditeurs internes des objectifs, de la conception, des opérations et de l'environnement de contrôle du domaine ou processus audité. Les organigrammes de l'organisation peuvent aider les auditeurs internes dans l'identification des parties prenantes concernées.

Les entretiens avec les directeurs des différents services peuvent servir à indiquer quels processus ont conduit à telle ou telle décision stratégique ou opérationnelle, à évaluer si les efforts déployés par l'organisation se traduisent par une sensibilisation suffisante à ses règles éthiques, et à vérifier si les collaborateurs ont une compréhension claire de leurs responsabilités relatives aux processus de management des risques et de contrôle, et des répercussions sur l'organisation.

Exemples de questions pour les entretiens :

- Quel est, selon le Conseil, le niveau de dépendance de l'organisation à l'égard des systèmes d'information ? Comment ce niveau de dépendance est-il reflété dans le plan stratégique ?
- Disposez-vous d'une définition claire de votre rôle en matière de gouvernance des SI ? Comment évaluez-vous que vous répondez aux attentes ?

- Quels organes de décision consultez-vous lors des prises de décision relatives aux systèmes d'information ?
- Quelles politiques sont en place et comment sont-elles diffusées par les différentes instances ou comités spécialisés de gouvernance ?
- Comment l'organisation mesure-t-elle la contribution des SI ?

Les auditeurs internes peuvent réaliser des *brainstorming* avec un collaborateur ou un groupe de collaborateurs pour identifier les risques pertinents. A cet effet, ils peuvent demander : « Qu'est-ce qui, selon vous, empêcherait l'atteinte des objectifs opérationnels ? » En outre, afin d'identifier les risques inhérents, les auditeurs peuvent demander : « Qu'arriverait-il si aucun contrôle n'était en place ? »

3. Réaliser une évaluation préliminaire des risques

En raison des contraintes de temps et de ressources, tous les risques ne peuvent pas être passés en revue pendant une mission. Par conséquent, les auditeurs internes sont tenus de réaliser une évaluation préliminaire des risques et de prioriser les risques en fonction de leur importance mesurée selon plusieurs facteurs de risques.

Pour des instructions détaillées sur l'élaboration de :

- scénarios de risques ;
- matrice des risques et des contrôles ;
- cartes de priorisation des risques (ex : carte des points critiques).

Consultez le Guide pratique de l'IIA « Planification de la mission : Définir les objectifs et le périmètre d'intervention ».

Une manière efficace de réaliser et de documenter une évaluation préliminaire des risques au niveau de la mission, est de créer un tableau présentant les risques et les contrôles pertinents sous forme, par exemple, d'une matrice des risques et des contrôles. Il s'agit d'un outil régulièrement utilisé par les auditeurs internes afin d'identifier, d'organiser et d'évaluer les risques pouvant impacter les objectifs opérationnels du domaine ou processus audité, ainsi que les contrôles visant à atténuer ces risques.

La **figure n°6** montre un exemple de matrice des risques et des contrôles utilisant les risques identifiés à partir de scénarios de risques. Dans cette matrice, les niveaux d'impact et de probabilité sont également inclus.

Figure 6 : Matrice des risques et des contrôles pour la gouvernance des SI

Scénarios de risques	Risque	Contrôle
Dans un modèle de fonctionnement décentralisé, les unités opérationnelles stratégiques sont autorisées à fonctionner de manière plus indépendante et autonome. Elles disposent de leurs propres budgets en matière de systèmes d'information et utilisent différentes applications et infrastructures SI.	L'organisation aura des difficultés à déployer efficacement à tous les niveaux un seul ensemble de normes pour les applications, l'infrastructure, les processus et les procédures SI.	L'architecture des systèmes d'information de l'entreprise devrait refléter la structure de l'organisation pour permettre un meilleur alignement et mieux répondre aux besoins de l'organisation. Le développement de la structure de gouvernance des SI devrait s'appuyer sur les conceptions d'architecture des systèmes d'information actuelles et anticipées.
L'organisation n'inclut pas le management des risques dans les pratiques de gestion de projet.	Les projets peuvent échouer à cause d'une mauvaise planification du traitement des risques.	Un processus est en place pour évaluer, traiter et communiquer aux parties prenantes clés et à la direction générale les risques associés aux SI pendant les processus de gestion de projet, de changement et de mise à jour.

L'Annexe D propose un exemple de matrice des risques et des contrôles pour la gouvernance des SI. Cette matrice fait office d'exemple et devrait être adaptée pour répondre aux besoins spécifiques de l'organisation auditée.

4. Définir les objectifs de la mission

Une fois que les auditeurs internes ont complété l'évaluation préliminaire des risques et identifié les risques significatifs à évaluer pendant la mission, ils peuvent définir les objectifs de la mission. Les objectifs de la mission précisent ce qu'il est prévu de réaliser pendant la mission et devraient, par conséquent, répondre à un but précis, concis et être en lien avec l'évaluation des risques (Normes 2210.A1).

Les objectifs de la mission pour la gouvernance des SI peuvent avoir trait à la conformité avec des exigences externes et internes en matière de gouvernance des SI, ou à la performance des processus de gouvernance des SI. Ils peuvent se définir de plusieurs manières. Par exemple, les objectifs peuvent être définis comme faisant partie du plan d'audit annuel, ou en tant que résultante de l'ERM *(Enterprise Risk Management),* de constats d'audits antérieurs, d'exigences réglementaires ou de besoins d'assurance spécifiques exprimés par le Conseil ou le comité d'audit.

Les auditeurs internes doivent également identifier les critères adéquats pour évaluer les processus de gouvernance, de management des risques et de contrôle au sein du domaine ou processus audité et pour déterminer si les objectifs opérationnels ont été atteints. L'identification de ces critères garantit que les objectifs de la mission d'assurance sont mesurables, réalistes et en cohérence avec les objectifs de l'organisation et du domaine ou processus audité.

Conformément à la Norme 2210.A3, les auditeurs internes doivent s'informer sur l'existence de critères établis par le management et/ou le Conseil. S'ils existent, ils doivent les utiliser. Si aucun critère n'a été défini, les

auditeurs internes doivent identifier, à travers une discussion avec le management et le Conseil, les critères d'évaluation appropriés. Les auditeurs devraient également envisager d'obtenir l'avis d'experts afin de développer les critères pertinents.

Exemples de critères :

- les indicateurs clés de performance en place ;
- les objectifs fixés pendant la planification stratégique ;
- le degré de conformité avec les règles et procédures du domaine ou processus, les lois et règlements externes et/ou des contrats ;
- les normes ou références du secteur.

Afin d'éviter les erreurs d'interprétation ou une remise en cause par les collaborateurs en charge du domaine ou processus audité, les critères d'évaluation devraient être pertinents, fiables et documentés. Ces critères adéquats et appropriés serviront de référence pour les auditeurs internes afin d'analyser les éléments probants, de comprendre les constats et d'évaluer l'adéquation des contrôles en place dans le domaine ou processus audité. Les critères, ou leur absence, devraient être comparés aux critères de références, tendances et prévisions du secteur, et aux règles et procédures de l'organisation.

Les exemples suivants indiquent que la fonction d'audit interne peut donner une assurance sur :

- l'adéquation des activités et des normes de gouvernance des SI avec l'appétence pour le risque de l'organisation telle que la fonction d'audit interne l'a comprise ;
- le traitement en temps utile des changements substantiels au niveau de l'organisation et des risques par l'instance de gouvernance des SI ;
- l'articulation et l'alignement des indicateurs et des objectifs SI avec les objectifs de l'organisation ;
- la mise en œuvre correcte des indicateurs pour une vision réaliste des opérations et de la gouvernance des SI tant au niveau tactique que stratégique.

4.1 Les objectifs de la mission de conseil

Les auditeurs internes peuvent intervenir sous différentes casquettes pour évaluer les pratiques de gouvernance et recommander des améliorations. Ils peuvent évaluer de manière indépendante et objective la conception et l'efficacité des processus de gouvernance au sein de l'organisation. En plus (ou au lieu) de fournir une assurance, les auditeurs internes peuvent choisir de donner des conseils.

Cette approche peut être privilégiée, plus particulièrement lorsque les problèmes sont identifiés ou que le processus de gouvernance est peu mature. Qu'il donne des conseils ou une assurance, le responsable de l'audit interne peut décider de recourir à des méthodes de contrôle en continu, en envoyant par exemple des auditeurs internes, en tant qu'observateurs, dans les réunions des instances en charge de la gouvernance pour y apporter des conseils au fur et à mesure, comme indiqué dans le Guide de mise en œuvre de la Norme 2110.

Dans la mesure où les missions de conseil sont par nature consultatives, les attentes et les objectifs sont déterminés par ou conjointement avec leur client donneur d'ordre. Par conséquent, la planification de la mission de conseil a généralement lieu après que les objectifs et le périmètre d'intervention de la mission ont été définis. Ainsi, les auditeurs internes n'ont pas besoin de réaliser une évaluation préliminaire des risques, comme

c'est le cas pour les missions d'assurance. Cependant, la Norme 2201.C1 stipule que les auditeurs internes doivent conclure avec le client donneur d'ordre un accord sur les objectifs et le périmètre d'intervention de la mission de conseil, les responsabilités de chacun et plus généralement sur les attentes du client donneur d'ordre. Pour les missions importantes, cet accord doit être formalisé.

En outre, les auditeurs internes doivent aborder les processus de gouvernance, de management des risques et de contrôle dans la limite convenue avec le client (Norme 2210.C1). Même si l'objectif et les attentes d'une mission de conseil sont définis par le client, les auditeurs internes doivent s'assurer que les objectifs de la mission sont en cohérence avec les valeurs, la stratégie et les objectifs de l'organisation (Norme 2210.C2).

Une mission d'analyse comparative (benchmark) pourra constituer un bon point de départ dans un plan d'audit pluriannuel, dans la mesure où elle laisse le temps à la direction de traiter les lacunes dans la conception de la structure de gouvernance avant que des examens supplémentaires ne soient effectués.

A travers des missions de ce type, l'audit interne pourra donner des conseils sur l'efficacité :

- des structures organisationnelles qui supportent la gouvernance des SI ;
- des contrôles de gouvernance existants en relation avec la gestion du changement.

5. Établir le périmètre d'intervention de la mission

Une fois que les objectifs fondés sur une approche par les risques ont été formulés, il est possible d'établir le périmètre d'intervention de la mission. Sachant qu'une mission ne peut généralement pas être exhaustive, les auditeurs internes doivent définir ce qui sera inclus ou non. Le périmètre d'intervention de la mission fixe les bornes de la mission et précise ce qui sera inclus dans l'audit. Les auditeurs internes devront apporter une attention particulière aux bornes de la mission pour s'assurer que le périmètre d'intervention sera suffisant pour atteindre les objectifs de la mission (Norme 2220 – Périmètre d'intervention de la mission).

Le périmètre d'intervention définit des éléments comme les processus et/ou les domaines spécifiques, les lieux géographiques, les périodes (par exemple : une période déterminée, un trimestre fiscal ou une année civile) couverts par la mission, compte tenu des ressources disponibles. Les auditeurs internes doivent considérer avec attention l'étendue du périmètre pour s'assurer qu'il permet une identification en temps opportun d'informations fiables, pertinentes et utiles permettant d'atteindre les objectifs identifiés de la mission (Norme 2210 – Objectifs de la mission et Norme 2310 – Identification des informations).

Lors de la définition du périmètre et de la réalisation d'une mission de gouvernance des SI, l'équipe d'auditeurs internes devrait :

- déterminer si la DSI s'aligne et comprend les objectifs et stratégies de l'organisation ;
- examiner la structure organisationnelle afin d'identifier si la fonction de DSI existe et si la personne occupant le poste est membre de la direction générale ;
- évaluer le niveau de cohérence des activités et des normes de gouvernance avec l'appétence pour le risque de l'organisation telle qu'elle a été comprise par la fonction d'audit interne ;
- déterminer l'efficacité des ressources et de la gestion de la performance des systèmes d'information ;
- évaluer les risques pouvant avoir un impact négatif sur l'environnement des systèmes d'information.

6. Affectation des ressources

Après avoir défini les objectifs et le périmètre d'intervention de la mission, les auditeurs internes doivent déterminer les ressources appropriées et suffisantes pour atteindre les objectifs de la mission, comme l'exige la Norme 2230 – Ressources affectées à la mission. L'interprétation de la Norme 2230 clarifie ce que l'on entend par ressources appropriées, c'est-à-dire la combinaison de connaissances, savoir-faire et autres compétences nécessaires à la réalisation de la mission ; par suffisantes, on entend la quantité de ressources nécessaires pour la réalisation de la mission avec conscience professionnelle.

Les ressources sont affectées à la mission en fonction des éléments suivants :

- les connaissances que les auditeurs internes acquièrent pendant la phase de planification de la mission ;
- la nature et la complexité de la mission ;
- les contraintes de temps et/ou le nombre d'heures budgétées pour la mission ;
- les connaissances, le savoir-faire et l'expérience des ressources disponibles.

Lorsque la fonction d'audit interne ne dispose pas des ressources appropriées et suffisantes, les auditeurs internes devraient considérer si des ressources (par exemple : des experts ou des ressources complémentaires) ou des technologies externes sont nécessaires.

7. Documenter le plan

Pendant la planification, les auditeurs internes formalisent les informations recueillies dans les documents de travail de la mission. Ces informations sont amenées à faire partie du programme de travail de la mission nécessaire à l'atteinte des objectifs de la mission, conformément à la Norme 2240 – Programme de travail de la mission.

Le processus de définition des objectifs et du périmètre d'intervention de la mission peut déboucher sur un ou plusieurs des documents de travail suivants :

- la cartographie du processus ;
- le résumé des entretiens et des séances de brainstorming ;
- l'évaluation préliminaire des risques (ex : matrice des risques et des contrôles et carte des points critiques) ;
- les explications des décisions qui ont abouti à la sélection des risques à inclure dans la mission ;
- les critères utilisés permettant d'évaluer le domaine ou processus audité (nécessaires pour les missions d'assurance conformément à la Norme 2210.A3).

La communication des résultats de la mission

Le style et le format de la communication des résultats de la mission varient selon les organisations et devraient tenir compte des lois et règlements, de la culture de l'organisation et des politiques de communication, ainsi que des attentes de la direction générale et du Conseil ou des instances de gouvernance équivalentes.

Parce que la gouvernance des SI est un élément stratégique pour toute la structure de gouvernance d'une organisation, il est important que le responsable de l'audit interne communique les résultats des audits de gouvernance des SI à la direction générale, au Conseil et au comité d'audit afin qu'ensemble, ils puissent traiter toute faiblesse apparente dans le cadre de l'exercice de leurs responsabilités respectives. La Norme 2060 – Communication à la direction générale et au Conseil stipule qu'il incombe au responsable de l'audit interne d'inclure dans cette communication les enjeux significatifs en matière de risques et de contrôle, dont les questions de gouvernance nécessitant l'attention de ces organes. La gouvernance des SI est essentielle à la structure et à la stratégie de toute l'organisation et les décideurs au plus haut niveau doivent être tenus informés lorsqu'ils envisagent l'incidence stratégique de la gouvernance des systèmes d'information pour toute l'organisation.

Se référer au Guide pratique de l'IIA : « Rapport d'audit : Communiquer les résultats d'une mission d'assurance » pour des lignes directrices détaillées sur la manière de préparer un rapport d'audit interne.

La gouvernance des SI vient en support des exigences réglementaires, légales, environnementales et opérationnelles de l'organisation permettant la réalisation des plans et des ambitions stratégiques. Aussi, est-il impératif que la direction générale, le Conseil et le comité d'audit soient informés en temps utile des résultats des missions d'audit de la gouvernance des SI.

Annexe A. Normes et lignes directrices de l'IIA applicables

Les *Normes internationales pour la pratique professionnelle de l'audit interne* pertinentes dans le cadre de ce guide pratique sont listées ci-dessous. Cette sélection n'est pas forcément exhaustive, seuls les passages des normes particulièrement pertinents pour ce guide sont repris. Veuillez vous référer aux Normes pour une citation complète. L'IIA conseille aux auditeurs internes de se référer au guide de mise en œuvre de chaque Norme.

Norme	Guide de mise en œuvre
1210 – Compétence	GM 1210 – Compétence
2000 – Gestion de l'audit interne	GM 2000 – Gestion de l'audit interne
2110 – Gouvernance	GM 2110 – Gouvernance
2130 – Contrôle	GM 2130 – Contrôle
2200 – Planification de la mission	GM 2200 – Planification de la mission
2201 – Considérations relatives à la planification	GM 2201 – Considérations relatives à la planification
2210 – Objectifs de la mission	GM 2210 – Objectifs de la mission
2220 – Périmètre d'intervention de la mission	GM 2220 – Périmètre d'intervention de la mission
2230 – Ressources affectées à la mission	GM 2230 – Ressources affectées à la mission
2400 – Communication des résultats	GM 2400 – Communication des résultats

Lignes directrices
Guide pratique, « Rapports d'audit : Communiquer les résultats d'une mission d'assurance », The IIA, octobre 2016
Guide pratique, « Planification de la mission : Définir les objectifs et le périmètre d'intervention », The IIA, août 2017
Guide pratique, « Planification de la mission : Evaluation des risques de fraude », The IIA, octobre 2017
Prise de position, « Les trois lignes de maîtrise pour une gestion des risques et un contrôle efficaces », The IIA, janvier 2013

Annexe B. Glossaire

Les termes marqués d'un astérisque (*) sont issus du glossaire du *Cadre de référence internationale des pratiques professionnelles* de l'IIA, édition 2017.

Appétence pour le risque* – Niveau de risque qu'une organisation est prête à accepter.

Audit interne* – Fonction assurée par un service, une division, une équipe de consultants ou tout autre praticien, c'est une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée. L'audit interne aide cette organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de gouvernance, de management des risques et de contrôle, en faisant des propositions pour renforcer leur efficacité.

Caractère significatif* – Niveau d'importance relative d'un évènement, dans un contexte donné et selon des facteurs d'appréciation qualitatifs et quantitatifs tels que la magnitude, la nature, l'effet, la pertinence et l'impact de cet évènement. Les auditeurs internes font preuve de jugement professionnel lorsqu'ils apprécient le caractère significatif des événements selon des objectifs pertinents.

Conformité* – L'adhésion aux règles, plans, procédures, lois, règlements, contrats ou autres exigences.

Conseil* – Le niveau le plus élevé des organes de gouvernance (par exemple, un conseil d'administration, un conseil de surveillance ou un organe délibérant) responsable du pilotage, et/ou de la surveillance des activités de l'organisation et, envers lequel la direction générale a un devoir de rendre compte. Bien que les mécanismes de gouvernance varient selon les juridictions et les secteurs, le Conseil comprend généralement des membres qui ne font pas partie du management. Si un tel Conseil n'existe pas, le mot « Conseil » dans les Normes correspond à un groupe ou à une personne en charge de la gouvernance de l'organisation. En outre, « Conseil » dans les Normes peut renvoyer à un comité ou une autre instance auquel l'organe de gouvernance a délégué certaines fonctions (par exemple, un comité d'audit).

Direction générale – Groupe de personnes détenant l'autorité déléguée par l'instance gouvernante pour la mise en œuvre des stratégies et politiques destinées à accomplir l'objectif de l'organisation. Ce groupe peut inclure des fonctions rattachées à l'instance de gouvernance ou au directeur de l'organisation ou qui ont un devoir de rendre compte global pour les grandes fonctions de responsabilité comme le directeur général, les chefs d'organisations gouvernementales, les directeurs des systèmes d'information (DSI) ou d'autres fonctions similaires.[3]

Gouvernance* – Le dispositif comprenant les processus et les structures mis en place par le Conseil afin d'informer, de diriger, de gérer et de piloter les activités de l'organisation en vue de réaliser ses objectifs.

[3] *Ibid 5.*

Gouvernance des systèmes d'information* – La gouvernance des systèmes d'information comprend la direction, les structures organisationnelles et les processus qui garantissent que les systèmes d'information soutiennent la stratégie et les objectifs de l'organisation.

Management – Réaliser des contrôles ou une supervision dans le cadre des pouvoirs et du devoir de rendre compte établis par une instance de gouvernance. Le terme management est souvent utilisé comme un terme générique pour désigner les personnes ayant la responsabilité de piloter tout ou partie d'une organisation.[4]

Mission d'assurance* – Il s'agit d'un examen objectif d'éléments probants, effectué en vue de fournir à l'organisation une évaluation indépendante des processus de gouvernance, de management des risques et de contrôle. Par exemple, des audits financiers, de performance, de conformité, de sécurité des systèmes ou de due diligence.

Mission de conseil* – Conseils et services y afférents rendus au client donneur d'ordre, dont la nature et le périmètre d'intervention sont convenus au préalable avec lui. Ces activités ont pour objectifs de créer de la valeur ajoutée et d'améliorer les processus de gouvernance, de management des risques et de contrôle d'une organisation sans que l'auditeur interne n'assume aucune responsabilité de management. Quelques exemples : avis, conseil, assistance et formation.

Norme* – Document professionnel promulgué par l'IIASB *(the International Internal Auditing Standards Board)* afin de définir les règles applicables à un large éventail d'activités d'audit interne et utilisables pour l'évaluation de l'audit interne.

Processus de contrôle* – Les règles, procédures et activités (aussi bien manuelles qu'automatisées) faisant partie d'un cadre de contrôle interne, conçues et mises en œuvre pour s'assurer que les risques sont maintenus dans les limites que l'organisation est disposée à accepter.

Responsable de l'audit interne* – « Responsable de l'audit interne » désigne une personne, occupant un poste hiérarchique de haut niveau, qui a la responsabilité de diriger efficacement la fonction d'audit interne conformément à la charte d'audit interne et aux dispositions obligatoires du Cadre de référence international des pratiques professionnelles de l'audit interne. Le responsable de l'audit interne ou des personnes qui lui sont rattachées de l'audit interne devront disposer des certifications et des qualifications professionnelles appropriées. L'intitulé exact du poste et/ ou de la fonction du responsable de l'audit interne varie selon les organisations.

Risque* – Possibilité que se produise un événement qui aura un impact sur la réalisation des objectifs. Le risque se mesure en termes de conséquences et de probabilité.

---

[4] *ISO/IEC 38500:2015, Technologies de l'information – Gouvernance des technologies de l'information pour l'entreprise, https://www.iso.org/obp/ui/#iso:std:iso-iec:38500:ed-2:v1:en.*

Annexe C. Questionnaire de contrôle interne relatif à la gouvernance des SI

Le questionnaire suivant a été conçu pour aider les auditeurs internes à évaluer, lors de la phase de planification de la mission, la situation de la gouvernance des SI.

Structures organisationnelle et de gouvernance

Les questions suivantes aideront l'auditeur interne à mieux comprendre le niveau ou l'existence de la gouvernance des systèmes d'information :

Question	Évaluation / Remarques
La fonction de DSI existe-t-elle et fait-elle partie de la direction générale ?	
La structure de l'organisation et ses composantes opérationnelles sont-elles clairement agencées de sorte que la fonction des SI puisse contribuer avec efficience et efficacité à l'atteinte des objectifs de l'organisation ?	
Des organes de décision sont-ils en place pour faciliter l'alignement des besoins de l'organisation sur les services SI et assument-ils les responsabilités et un devoir de rendre compte adéquats?	
Les besoins de l'organisation et les exigences en matière de services SI sont-ils définis dans les plans stratégique et tactique et surveillés ?	
Le DSI et la direction générale se réunissent-ils de manière régulière pour discuter des progrès réalisés ?	
Les rôles et responsabilités sont-ils clairement définis et communiqués et les dirigeants de l'organisation sont-ils responsabilisés et tenus de rendre compte des résultats ?	

Leadership et soutien de l'exécutif

Les questions suivantes aideront l'auditeur interne à mieux comprendre le niveau d'intégration de la gouvernance des systèmes d'information au sein de l'organisation :

Question	Évaluation / Remarques
La direction générale a-t-elle clairement défini et communiqué les rôles et responsabilités de la fonction SI en lien avec les objectifs stratégiques et tactiques de l'organisation ?	
Les rôles et responsabilités du DSI sont-ils clairement définis et communiqués ?	
L'organisation reconnaît-elle dans sa stratégie que la fonction SI contribue de manière significative à l'atteinte des objectifs et qu'elle soutient l'organisation au quotidien ?	
Le DSI se réunit-il régulièrement avec la direction générale et le Conseil pour débattre des prestations SI en lien avec les plans stratégique et tactique ?	
La fonction des SI dispose-t-elle du financement adéquat pour répondre aux besoins de l'organisation ?	

Planification stratégique et opérationnelle

En posant les questions suivantes, l'auditeur interne pourra se faire une idée du niveau de mise en œuvre du management de la performance stratégique par la direction générale :

Question	Évaluation / Remarques
Le Conseil et la direction générale considèrent-ils que les SI font une contribution stratégique à l'organisation ?	
Le plan stratégique de l'organisation explique-t-il comment les SI peuvent soutenir et contribuer à la création de valeur ?	
Le plan stratégique est-il soutenu par des plans opérationnels tactiques intégrant les exigences et les livrables des SI ?	
Existe-il des indicateurs clés de performance (KPI) utilisés par la direction générale pour mesurer et surveiller l'efficacité de la fonction SI ?	
Les décisions en matière d'investissements stratégiques pour les SI s'appuient-elle sur des analyses de rentabilité et sont-elles évaluées a posteriori pour définir si le retour sur investissement prévu s'est bien produit ?	
Les retours d'expérience sont-ils pris en compte en matière d'investissements SI ?	
L'organisation des SI est-elle structurée efficacement en fonction de la taille et de la composition de l'organisation ?	
Le DSI et l'équipe de direction de la fonction SI sont-ils qualifiés et expérimentés ?	

Prestation de service et suivi de la performance

En posant les questions suivantes, l'auditeur interne pourra comprendre le niveau de fonctionnement de la gestion financière des SI :

Question	Évaluation / Remarques
Le Conseil et la direction générale ont une compréhension précise des coûts des SI et de la manière dont ils contribuent à l'atteinte des objectifs stratégiques de l'organisation ?	
Les dirigeants de l'organisation mesurent-ils la valeur et les livrables des systèmes d'information ? Si oui, comment ?	
Quels sont les résultats de la comparaison des coûts liés aux SI avec des organisations similaires ?	
La performance du DSI est-elle mesurée à l'aune de données financières et extra-financières ?	
Des dispositifs de gestion des ressources sont-ils en place ? Si oui, sont-ils évalués et suivis ?	

Organisation et management des risques SI	
En posant les questions suivantes, l'auditeur interne pourra se faire une idée précise de l'environnement de la gouvernance des SI :	
Question	**Évaluation / Remarques**
Dans quelle mesure les processus de l'organisation sont-ils automatisés ?	
Quel est le degré de complexité de l'infrastructure SI et combien d'applications sont utilisées ?	
Les données sont-elles normalisées et aisément partagées entre les applications (et au sein de l'infrastructure SI) ?	
Le matériel informatique, les logiciels, les politiques, procédures et contrôles des services sont-ils normalisés ?	
Quelle est la maturité des processus de gestion des SI et des cadres de référence reconnus sont-ils utilisés (ex : COBIT, ITIL, ISO) ?	
Comment les risques sont-ils gérés en relation avec les besoins et les exigences en matière de sécurité et de conformité de l'organisation ?	
Quelle est l'importance stratégique des SI ?	

Annexe D. Matrice des risques et des contrôles relative à la gouvernance des SI

Cette annexe propose des exemples d'objectifs métiers, de risques et de contrôles afin d'aider les auditeurs internes à élaborer le programme de travail de la mission.

Structures organisationnelle et de gouvernance	
Objectif de contrôle : Les structures organisationnelles devraient inclure des liens hiérarchiques, des rôles et des responsabilités clairement définis.	
Risque	Contrôle
Le devoir de rendre compte n'est pas clairement défini et débouche sur un manque de transparence au niveau des coûts, des processus, des projets et des services liés aux SI.	Les objectifs et buts stratégiques de l'organisation devraient sous-tendre les objectifs et les cibles métier. De même, la responsabilité de l'atteinte des objectifs devrait revenir aux responsables des unités opérationnelles afin de promouvoir un devoir de rendre compte explicite.
L'absence de responsabilisation ou de devoir de rendre compte se traduit par des opportunités ratées en matière d'innovation et de collaboration.	Les personnes en charge des SI et des unités opérationnelles devraient être responsabilisées pour gérer les ressources au sein de leur domaine de responsabilité et ainsi les diriger vers les objectifs de performance escomptés.
L'alignement stratégique et la compréhension entre les fonctions métiers et SI sont confus causant une contribution amoindrie aux bénéfices des parties prenantes.	La création de structures organisationnelles pluridisciplinaires permet de représenter les différents intérêts au sein de l'organisation. L'audit interne y représente les intérêts de toute l'organisation.
La direction générale et le Conseil ne comprennent pas la relation entre les SI et les objectifs métiers et cela peut déboucher sur une affectation inefficace des ressources pour des initiatives stratégiques et/ou sur une mauvaise compréhension des coûts généraux liés aux SI et de leur contribution aux retours sur investissement.	Les rôles et responsabilités devraient fournir des dispositifs destinés à coordonner l'usage des SI et les stratégies et objectifs globaux de l'organisation.
Objectif de contrôle : Les structures organisationnelles précisent la nature opérationnelle de leurs composantes et les protocoles de communication.	
Risque	Contrôle
Les canaux de communication entre la fonction SI et les responsables d'unités opérationnelles sont flous ce qui conduit à un système de planification et de surveillance inefficace.	Pour des actions cohérentes dans toute l'organisation, une communication efficace continue autour de la gouvernance des SI devrait avoir lieu dans toutes les unités et pour toutes les fonctions. Un plan de communication en bonne et due forme devrait reprendre les aspects et indicateurs nécessaires pour être avisé, les préparateurs et les destinataires, une fréquence et des procédures de recours hiérarchique.

Structures organisationnelle et de gouvernance

Objectif de contrôle : Les collaborateurs de la fonction SI sont capables d'allouer les ressources nécessaires à l'atteinte des objectifs métiers.	
Risque	**Contrôle**
Les rôles et responsabilités au niveau de la fonction SI sont flous débouchant sur une discordance entre les ressources et les objectifs opérationnels.	Les processus, rôles et responsabilités des collaborateurs des SI sont définis, documentés et communiqués.
L'usage des ressources et actifs SI est irresponsable en l'absence de processus SI cohérents et reproductibles.	Les processus sont documentés et évalués périodiquement pour assurer leur cohérence et reproductibilité.
Objectif de contrôle : Les métiers et les SI collaborent autour des ressources, priorités, initiatives et décisions générales d'investissement.	
Risque	**Contrôle**
L'équipe de direction de la fonction SI n'est pas incluse dans le processus décisionnel d'alignement des SI sur les objectifs de l'organisation ce qui génère l'incapacité des SI à soutenir les décisions ou à s'adapter en temps utile aux priorités changeantes.	La direction générale et le Conseil devraient incorporer les SI dans les décisions stratégiques en matière de gouvernance, permettant aux SI d'ajouter de la valeur pour les décisions clés.
Le manque ou la mauvaise qualité des processus de gestion du portefeuille des SI peut générer une mauvaise priorisation des investissements en matière de SI.	Un processus solide de gestion du portefeuille est en place et permet à l'organisation et aux SI de collaborer autour des ressources, priorités, initiatives et décisions générales d'investissement.
Il existe une discordance entre les ressources SI et les objectifs opérationnels débouchant sur un mécontentement des parties prenantes internes et externes (gouvernements, régulateurs, société en général, actionnaires, Conseil, associés, clients, fournisseurs, consultants, collaborateurs et auditeurs externes) par rapport au fonctionnement de l'organisation et aux résultats financiers.	Les responsables d'unités opérationnelles se réunissent avec le DSI et d'autres responsables de la fonction des SI afin de déterminer les méthodes les plus efficaces pour soutenir et contribuer aux objectifs de chaque unité opérationnelle.
Objectif de contrôle : La structure de gouvernance des SI est définie en harmonie avec l'architecture SI (par exemple, si le management stratégique est centralisé au siège, la structure de gouvernance devrait l'être également).	
Risque	**Contrôle**
Une architecture d'entreprise inadaptée peut générer un investissement inutile dans des technologies redondantes et incompatibles.	L'architecture des systèmes d'information de l'entreprise devrait refléter la structure de l'organisation pour permettre un meilleur alignement et mieux répondre aux besoins de l'organisation.
Une discordance entre la structure de gouvernance des SI et l'architecture SI peut déboucher sur des processus qui ne soutiennent pas les besoins de l'organisation et sont trop coûteux à modifier.	Le développement de la structure de gouvernance des SI devrait s'appuyer sur les conceptions d'architecture SI actuelles et anticipées.

Leadership et soutien de la direction

Objectif de contrôle : La vision, la mission et la stratégie de l'organisation fournissent collectivement l'orientation des investissements en matière de SI.	
Risque inhérent	**Contrôle**
Une absence de vision, de mission et de plan stratégique clairs pour l'organisation et le rôle des SI peut générer un usage inefficace du capital SI et d'autres ressources nécessaires à l'atteinte des objectifs stratégiques de l'organisation.	La vision de l'organisation est la base pour définir les cadres de référence, processus, activités, rôles et relations. La vision devrait être documentée sous la forme d'un plan stratégique définissant la dépendance aux SI.
Il n'existe aucune relation claire entre les indicateurs de performance de projet SI et les objectifs de l'organisation.	Les objectifs et les indicateurs de l'organisation et des SI sont alignés.
La direction générale n'est pas correctement impliquée dans le processus de décision des SI ce qui peut se traduire par une mauvaise affectation des ressources des SI.	Les rôles sont établis, communiqués et acceptés explicitement pour la prise de décision en matière d'investissement, le financement et la gestion du programme, la gestion du projet, la prestation de services et les rôles de support associés.
Une absence de définition de la valeur et du coût des SI en termes d'impact sur les objectifs de l'organisation peut aboutir sur une incapacité des SI à atteindre leurs propres objectifs, ainsi que les objectifs stratégiques globaux de l'organisation.	Une formation formelle est à prévoir pour informer les propriétaires et les administrateurs. Cette formation devrait être obligatoire lors du processus d'intégration d'un collaborateur, puis suivie de sessions périodiques afin d'expliquer les changements de politique et leur incidence sur les pratiques de travail.
Objectif de contrôle : Le budget lié aux SI est communiqué à la direction générale.	
Risque inhérent	**Contrôle**
La direction générale n'est pas au courant du financement des SI et de ses implications sur les ressources de l'organisation.	Les budgets sont régulièrement mis à jour et communiqués.
Objectif de contrôle : Les budgets sont contrôlés et surveillés.	
Risque inhérent	**Contrôle**
Les budgets liés aux SI sont réaffectés à des projets non-stratégiques sans révision et approbation formelle.	Les pratiques de planification financière des SI sont régulièrement analysées et les ressources sont réaffectées systématiquement lorsque la documentation et l'approbation correspondantes sont fournies.
Les dépenses liées aux SI ne sont pas alignées sur les objectifs métiers pouvant aboutir sur une affectation des ressources vers des objectifs secondaires.	Demander au management de fournir une analyse de rentabilité et les calculs des retours sur investissement de projets d'investissements SI pour aider le Conseil et la direction générale à prendre les meilleures décisions possibles.

Leadership et soutien de la direction

Objectif de contrôle : La direction comprend les investissements réalisés en matière de SI.	
Risque inhérent	**Contrôle**
La direction générale et les responsables d'entités opérationnelles ne comprennent pas les SI, ce qui peut déboucher sur des opportunités manquées et de moindres retours sur investissement.	Afin de réduire la probabilité de mauvaises décisions en matière d'investissements en SI, les dirigeants de l'organisation devraient comprendre les caractéristiques premières des SI. À cet égard, le DSI est invité aux réunions du Conseil afin de débattre des risques et opportunités associés aux SI.
L'absence de vision globale de l'organisation de la part de l'équipe de direction de la fonction SI pourrait amener celle-ci à ne pas canaliser ses efforts ou à faire un mauvais usage des ressources.	La direction générale et le Conseil devraient avoir une compréhension précise des objectifs et des stratégies clés.

Objectif de contrôle : Les initiatives SI sont alignées sur les objectifs de l'organisation.	
Risque inhérent	**Contrôle**
L'importance stratégique des SI n'est pas évaluée générant une mauvaise compréhension du rôle des SI dans l'organisation.	Les dirigeants de la fonction SI et de l'organisation se réunissent régulièrement pour passer en revue les initiatives présentes et futures des SI afin de réévaluer l'alignement sur les objectifs de l'organisation (ex : évaluer la validité de la documentation du business case).
Les ressources SI sont affectées à des objectifs secondaires.	

Objectif de contrôle : La gouvernance des SI contribue à relancer l'innovation au niveau des systèmes d'information et de l'ensemble de l'organisation.	
Risque inhérent	**Contrôle**
Un manque d'engagement de la part des dirigeants exécutifs peut amener à une promotion inappropriée de l'innovation au niveau des systèmes d'information et de l'ensemble de l'organisation.	L'engagement des dirigeants est démontré par des initiatives soutenant la stratégie SI.

Planification stratégique et opérationnelle

Objectif de contrôle : Les stratégies SI et métiers sont alignées.	
Risque inhérent	**Contrôle**
L'alignement stratégique et la compréhension entre les fonctions métiers et SI sont confus causant : ■ une contribution amoindrie aux bénéfices des parties prenantes ; ■ une affectation inefficace des ressources aux initiatives stratégiques ; ■ un manque de transparence au niveau des coûts, processus, projets et services des systèmes d'information ; ■ une mauvaise compréhension des coûts généraux des SI et de leur contribution aux retours sur investissement.	Les responsabilités et pratiques sont documentées dans des cadres de référence de gouvernance. Le DSI participe aux réunions du Conseil et la contribution des SI aux objectifs de l'organisation est discutée.
Des structures organisationnelles floues et/ou inadaptées peuvent générer : ■ une mauvaise gestion des ressources et des activités contradictoires ; ■ une discordance entre les ressources et les objectifs opérationnels ; ■ un mécontentement des parties prenantes externes et internes quant au fonctionnement de l'organisation.	Le cadre de référence de gouvernance est organisé en processus et comprend des informations autour des activités, des propriétaires et domaines d'amélioration des processus.
Des canaux de communication flous entre les SI et les responsables d'unités opérationnelles se traduisent par un système de planification et de surveillance inefficace.	L'organisation stratégique devrait inclure des protocoles de communication pour s'assurer que les SI et les métiers entretiennent un dialogue ouvert.

Objectif de contrôle : L'organisation a défini des rôles qui reprennent le devoir de rendre compte, les niveaux d'autorité et les droits de décision.	
Risque inhérent	**Contrôle**
L'usage des ressources et des actifs SI est irresponsable par manque de processus SI cohérents et reproductibles.	Des descriptifs formalisés des postes et des rattachements ont été créés et communiqués à tous les niveaux de la fonction SI. Les processus sont correctement documentés, publiés et les collaborateurs savent où les trouver.
Les investissements et des priorités en matière de SI ne sont pas alignés sur les objectifs métiers.	La stratégie des SI est documentée et mise à jour régulièrement afin d'y intégrer les attentes des parties prenantes.

Objectif de contrôle : L'allocation des ressources SI correspond aux objectifs stratégiques.	
Risque inhérent	**Contrôle**
Une affectation des ressources inadaptée pour la prestation des services SI requis ne permettra pas d'obtenir de bénéfices technologiques, fera manquer des opportunités ou entravera l'atteinte des objectifs de l'organisation.	Les ressources (collaborateurs, applications, matériel) ont été affectées pour soutenir les objectifs de l'organisation.

Prestation de service et suivi de la performance

Objectif de contrôle : Les systèmes d'information correspondent aux plans, budgets et engagements.	
Risque inhérent	**Contrôle**
Les principaux processus de l'activité subissent l'incidence négative de mauvaises prestations de service SI.	Des processus sont en place pour réviser les indicateurs clés de performance et corriger les éléments se trouvant en dessous du seuil raisonnable.
Objectif de contrôle : La fonction SI partage les indicateurs de performance avec les parties prenantes clés.	
Risque inhérent	**Contrôle**
La direction générale et le Conseil ne disposent pas d'une vision claire de la performance SI sur base de données quantifiables.	Un plan de communication en bonne et due forme devrait reprendre les aspects et indicateurs nécessaires pour être avisé, les préparateurs et les destinataires, une fréquence et des procédures de recours hiérarchique.
L'atteinte des objectifs stratégiques n'est pas surveillée ou communiquée.	Les objectifs stratégiques sont atteints au lieu d'être modifiés ou manqués.
Les activités de gestion de la performance n'incluent pas d'indicateurs relatifs aux tiers.	Les activités de gestion de la performance considèrent les activités des SI internes et des tiers.
Une absence de capacité d'analyse en cascade pour des indicateurs des niveaux inférieurs peut déboucher sur : ■ un retour sur investissement en matière de SI qui n'est pas surveillé ; ■ une absence d'information destinée à la prise de décision ; ■ des coûts supérieurs aux entités comparables.	Le reporting financier devrait être défini avec suffisamment de détails pour permettre des capacités d'analyse en cascade et d'analyse des coûts.
Un manque de données financières précises peut générer une mauvaise traçabilité de la valeur créée par les SI.	Les données financières associées aux investissements en matière de SI sont captées et transmises aux parties prenantes.
Objectif de contrôle : La performance SI est communiquée avec une terminologie partagée par la fonction SI et les métiers.	
Risque inhérent	**Contrôle**
Les rapports des SI sont préparés dans le jargon des SI.	Les rapports de performance des SI doivent être structurés de manière à être compris par toutes les parties prenantes, des SI ou non.
Objectif de contrôle : Les indicateurs s'appuient sur les besoins métiers changeants.	
Risque inhérent	**Contrôle**
Des indicateurs de performance flous ne permettent pas de rendre compte de l'état précis des initiatives SI.	Des indicateurs de performance sont définis avec des éléments de mesure et de comparaison.

Organisation et management des risques SI

Objectif de contrôle : Le niveau de risques associés aux SI que l'organisation est prête à accepter pour atteindre ses objectifs est défini («risk appetite» ou appétence pour le risque).	
Risque inhérent	Contrôle
Les risques associés aux SI dépassent l'appétence pour le risque de l'organisation.	L'organisation assure un suivi du management des risques et des activités de contrôle associés aux SI.
Les risques associés aux SI dépassent la tolérance au risque de l'organisation.	Les évaluations et les scénarios de risques sont mis à jour régulièrement et les résultats sont correctement communiqués.
Les risques associés aux SI ne sont pas intégrés dans le système de management des risques à l'échelle de l'organisation (ERM - *Enterprise Risk Management)*.	La stratégie de management des risques de l'organisation reprend les risques associés aux SI.
L'information relative aux risques et au contrôle n'est pas communiquée aux secteurs appropriés de l'organisation, ce qui peut déboucher sur des décisions prises au-delà des limites de tolérance au risque de l'organisation.	Un processus est en place pour évaluer, traiter et communiquer aux parties prenantes clés et à la direction générale les risques associés aux SI pendant les processus de gestion de projet, de changement et de mise à jour.
Objectif de contrôle : Un plan de continuité d'activité et de reprise après sinistre est en place et est régulièrement testé.	
Risque inhérent	Contrôle
L'organisation fait face à d'importantes violations de la sécurité des données ce qui génère des réactions négatives des clients et nuit à l'image de marque de l'organisation.	L'organisation a mis en place un processus pour gérer de manière proactive les risques, les menaces, les changements et les imprévus importants.
Objectif de contrôle : Les projets SI sont achevés dans les délais et en respectant le budget.	
Risque inhérent	Contrôle
Les processus de gestion de projet n'incluent pas d'évaluation des risques.	Un plan de management des risques est en place et les activités de management des risques sont incorporées aux processus de gestion de projet, de changement et de mise à jour.
Objectif de contrôle : Le profil de risque des SI est mis à jour régulièrement.	
Risque inhérent	Contrôle
Le profil de risque des SI n'est pas géré correctement et des risques ne sont pas traités ou se situent au-delà des limites de tolérance.	Le profil de risque des SI est mis à jour dans le cadre des bonnes pratiques du système de management des risques de l'entreprise.

Organisation et management des risques SI

Objectif de contrôle : La classification des actifs détermine le niveau de contrôle nécessaire pour leur traitement et leur utilisation.	
Risque inhérent	Contrôle
Les données relatives aux collaborateurs ou aux clients peuvent être divulguées ou accessibles par des parties internes ou externes non autorisées.	Les détails de la classification, de l'usage, de l'origine et de la localisation devraient être repris dans un registre des actifs. Ceci devrait être réalisé par les administrateurs des SI.
Le registre des actifs n'est pas mis à jour pour refléter de nouveaux risques, menaces ou vulnérabilités.	Les processus destinés à tenir le registre à jour doivent être développés et mis en place pour identifier en continu les domaines où les risques sont les plus élevés.
Objectif de contrôle : Les systèmes d'incitation de l'organisation sont conçus et exécutés pour prévenir ou détecter les comportements inacceptables.	
Risque inhérent	Contrôle
Un management incohérent de la performance et du devoir de rendre compte peut provoquer des actions qui ne soutiennent pas les objectifs stratégiques.	L'organisation a mis en œuvre des politiques et des processus de rémunération des collaborateurs, de définition des objectifs et d'évaluation de la performance.
Un comportement inacceptable ou une prise de risques excessive n'est pas détecté(e).	Les éléments de mesure associées (ex : indicateurs clés de performance) et les systèmes incitatifs (ex : primes) sont correctement conçus et exécutés pour prévenir ou détecter un comportement inacceptable ou une prise de risques excessive et soutenir les actions alignées sur les objectifs stratégiques de l'organisation.

Annexe E. Ressources supplémentaires

The Committee on the Financial Aspects of Corporate Governance, *Financial AspectsApp of Corporate Governance* (The Cadbury Report), 1992. http://www.ecgi.org/codes/documents/cadbury.pdf

Le *COBIT* est un cadre de référence pour la gouvernance des SI en entreprise publié par l'ISACA en 2012. www.isaca.org/cobit/pages/default.aspx

Organisation internationale de normalisation (ISO) / Commission électrotechnique internationale (IEC – *International Electrotechnical Commission*) 38500:2015, *Governance of IT for the Organization*, la version de 2015 est un cadre de référence pour la gouvernance des SI et une contribution clé pour d'autres cadres de référence comme l'ITIL et le COBIT.
https://www.iso.org/standard/62816.html

L'*IT Infrastructure Library* (ITIL) est un cadre de référence développé par le Cabinet du premier ministre du Royaume Uni en tant que bibliothèque regroupant les meilleures pratiques pour le management des systèmes d'information. https://www.itil-itsm-world.com/index.htm

King Report on Corporate Governance and King Code of Corporate Governance (King III) de L'*Institute of Directors in Southern Africa* (IoDSA), a été compilé par le King Committee en réponse à l'émergence de la Loi *South African companies Act 71* de 2008. Un nouveau King IV a été publié le 1er novembre 2016. http://www.iodsa.co.za/?kingIII

National Computing Centre, *IT Governance: Developing a successful governance strategy,* NACD 2005.

NIST SP 800-39, *Managing Information Security Risk : Organization, Mission, and Information System View,* NIST 2011.

Organisation de coopération et de développement économiques (OCDE) *Principes de gouvernance d'entreprise du G20 et de l'OCDE,* version 2015

Remerciements

Équipe de projet

Himi Tina Kim CIA, CGAP, CRMA, États-Unis (Chairman)
Avin Mansookram, Afrique du Sud (Project Lead)
Kenneth Drinkard, États-Unis
Sajay Rai, États-Unis
Terence Washington, CIA, CRMA, Etats-Unis

Contributeurs

Harun Abdul Haqq, CIA, CISA, CFE, Trinité-et-Tobago
Graciela Braga, CGEIT, CSX (F), Argentine
Jason Brucker, CISA, CGEIT, États-Unis
Elastos Chimwanda, CIA, CISA, Zimbabwe
Jamie DuBray, CIA, CRMA, CISA, CGEIT, CISSP, États-Unis
Ulrich Hahn, CIA, CGAP, CRMA, CISA, Allemagne
Nigel James, CISA, Etats-Unis
Stephen Stanbury, CIA, CRMA, CFE, Royaume-Uni

Collaborateurs de l'IIA Global en charge des Normes et des lignes directrices

Eva Sweet, Director (Project Lead)
Lisa Hirtzinger, CIA, QIAL, CCSA, CRMA, Vice President
Debi Roth, CIA, Managing Director
Lauressa Nelson, Technical Writer
Michael Citro, Technical Writer

Réviseurs de la traduction française

Bruno Buresi, CISA
Vianney Dumont, CIA
Christophe Butikofer, CIA
Julien Cornuché, CIA, CISA
Béatrice Ki-Zerbo, CIA
Sébastien Lepers, CIA, CFE, CGAP, CRMA

L'IIA aimerait remercier les organes de surveillance suivants pour leur soutien : Information Technology Guidance Committee, Professional Guidance Advisory Council, International Internal Audit Standards Board, Professional Responsibility and Ethics Committee, and International Professional Practices Framework Oversight Council.

À propos de l'IIA

Porte-parole mondial de la profession d'audit interne, l'*Institute of Internal Auditors* (IIA) est une autorité reconnue et un leader incontesté dans la formation et la formulation de normes, lignes directrices et certifications. Fondé en 1941, l'IIA, dont le siège mondial se situe à Lake Mary (Floride, États-Unis), compte actuellement quelque 190 000 membres dans plus de 170 pays et territoires. Plus d'informations sont disponibles sur le site www.globaliia.org / www.theiia.org.

Avertissement

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

Copyright

Copyright© 2018 *The Institute of Internal Auditors, Inc.* Tous droits réservés. Pour l'autorisation de reproduction, prière de contacter l'*Institute of Internal Auditors* à l'adresse guidance@theiia.org ou l'IFACI à l'adresse recherche@ifaci.com

Janvier 2018 – ISBN: 978-2-915042-87-0

The Institute of Internal Auditors | Global

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101
www.theiia.org