BUREAU DU VÉRIFICATEUR GÉNÉRAL DU CANADA

GUIDE D'AUDIT DE PERFORMANCE

GUIDE POUR EFFECTUER

UN AUDIT DE LA GESTION DE L'INFORMATION ET DE LA TECHNOLOGIE DE L'INFORMATION

MAI 2014

TABLE DES MATIÈRES

INTRODUCTION

Le présent Guide fait partie d'une série de guides préparés à l'intention des auditeurs pour les aider à effectuer l'examen de divers systèmes et pratiques dans le cadre d'un audit de performance. Il définit les connaissances sur la gestion de l'information et la technologie de l'information (GI/TI) qui sont nécessaires pour effectuer des audits de performance au BVG.

Qu'est-ce que la GI/TI (gestion de l'information et technologie de l'information)?

La gestion de l'information (GI) est un élément essentiel des activités opérationnelles d'une entité. Elle joue un rôle central pour assurer la protection de l'information de nature délicate et faire en sorte que les ressources informationnelles importantes pour la réalisation du mandat et des objectifs opérationnels d'une entité sont facilement accessibles. Cette information est généralement gérée au moyen d'une fonction de technologie de l'information (TI), chargée de diriger et de soutenir une gestion de l'information efficace et efficiente, comme la planification et le développement des systèmes, et l'élimination de l'information ou sa conservation à long terme. La fonction de TI veille à protéger la confidentialité, l'intégrité et la disponibilité de l'information qui est essentielle à la prise de décisions et à la prestation des services du gouvernement. Grâce à de bonnes pratiques de tenue des documents, les ministères peuvent créer, acquérir, saisir et gérer les ressources informationnelles possédant une valeur opérationnelle pour l'exécution des programmes et la prestation des services du gouvernement du Canada tout en protégeant leur intégrité.

Les ministères et organismes du gouvernement fédéral utilisent quotidiennement la TI (Internet, ordinateurs, téléphones cellulaires, appareils mobiles) pour rehausser leur productivité, communiquer, collaborer et améliorer la prestation des services à la population canadienne. Dans toute entité (société d'État, organisme ou ministère), la masse d'informations utilisées pour diriger l'organisation est enregistrée, générée ou gérée sur un système de GI. La GI et la TI s'unissent pour assurer la collecte, l'enregistrement et la gestion de l'information dont les entités ont besoin pour fonctionner et prendre les décisions opérationnelles.

Pourquoi est-ce important d'auditer la GI/TI?

Les systèmes de GI/TI font en général partie intégrante de la gestion de l'entité, qui doit pouvoir compter sur une information de qualité pour prendre ses décisions de nature opérationnelle. Produire une valeur pour les parties intéressées exige une bonne gouvernance et une bonne gestion des actifs liés à l'information et à la technologie. Les conseils, les dirigeants et la direction de l'entité doivent traiter la GI/TI comme n'importe quel autre secteur important de leurs activités.

Aux termes de la politique du Conseil du Trésor, les entités se doivent de gérer efficacement leur information, et, pour se conformer aux normes d'audit, les équipes d'audit de performance doivent posséder une compréhension de la technologie de l'information pertinente. L'équipe d'audit qui définit et audite divers cadres, systèmes et pratiques de l'entité en rapport avec la gestion de l'information ajoutera de la valeur si elle s'intéresse aux résultats plutôt qu'uniquement aux politiques et aux méthodes.

Pour réaliser un audit de performance exhaustif et utile, les auditeurs doivent connaître les risques importants en GI et en TI à considérer lorsqu'ils auditent une entité, un secteur ou le gouvernement. Les auditeurs devraient intégrer les travaux et questions d'audit connexes dans les secteurs d'examen compris dans l'étendue de leur audit.

Comment l'audit de la GI/TI soutient-il les autres travaux d'audit du BVG?

Les audits du BVG font souvent largement confiance aux systèmes et aux données de l'entité pour sonder et choisir les éléments à examiner. En intégrant l'examen de la GI/TI dans les audits de performance, les auditeurs du BVG pourront acquérir un certain degré de confiance à l'égard des systèmes et des données des entités, sur lesquelles ils pourront s'appuyer pour la conduite de leurs travaux.

OBJECTIFS DU GUIDE

Le présent guide indique aux auditeurs comment :

- intégrer efficacement la GI/TI dans les secteurs d'intérêt d'un audit de performance d'une entité, d'un secteur ou du gouvernement;
- découvrir les connaissances au sujet de la GI/TI qu'ils doivent posséder pour cerner efficacement les enjeux potentiels en la matière au moment de planifier leur audit, de préparer et d'actualiser leurs plans d'audit, et de préparer leurs propositions de chapitre.

Les objectifs du Guide sont les suivants :

- exposer une méthode d'audit de performance améliorée, axée sur la prestation des services de la GI/TI;
- aider les auditeurs à comprendre et à recenser les possibilités d'inclure la GI/TI dans l'étendue de l'audit au début de l'étape de la planification ou même avant, selon le profil de risque d'entreprise de l'entité, ses plans d'activités intégrés, ses rapports ministériels sur le rendement, ses rapports sur les plans et les priorités et d'autres documents connexes;
- déterminer à quel moment il y aurait lieu de recourir aux connaissances spécialisées de l'équipe de la prestation des services et des technologies de l'information du BVG.

CONNAISSANCE DE LA GI/TI

Connaissances requises en GI/TI

Par le truchement de la section 3061 du Manuel d'audit de performance du BVG, le Bureau suit le Manuel de CPA Canada — Certification qui se rapporte aux audits de performance. Ces normes exigent que les auditeurs possèdent une connaissance et une expertise techniques, y compris la connaissance de la technologie de l'information pertinente[1]. De

[1] Manuel de CPA Canada — Certification :
- Normes canadiennes de contrôle qualité — NCCQ 1, paragraphe A31;
- Autres normes canadiennes — chapitre 5030, paragraphe 24.

plus, les auditeurs devraient tenir compte de la Politique sur la gestion de l'information qui impose aux entités de gérer effectivement l'information en :

1. permettant un accès pratique à de l'information pertinente, fiable, complète et en temps opportun pour les programmes et les services du gouvernement;
2. soutenant les résultats des programmes et des services et en satisfaisant aux besoins opérationnels et aux obligations de rendre des comptes;
3. mettant en place des structures, des mécanismes et des ressources de gouvernance.

Importance de comprendre la GI/TI dans le contexte des audits de performance

Le Bureau réalise des audits de performance essentiellement sur les sujets choisis pour les programmes et les secteurs mentionnés dans le plan stratégique des audits (PSA). Le PSA expose les sujets d'audit à venir considérés comme présentant les risques les plus élevés.

Bien comprendre un sujet d'audit suppose de connaître les activités : le directeur principal de l'audit d'une entité acquiert, entretient, communique et documente les connaissances à jour au sujet de l'entité, notamment les risques qui pèsent sur elle. Cela couvre les principaux systèmes de TI qui génèrent l'information sur laquelle repose la prise de décisions de la haute direction de l'entité.

Les coûts de la GI/TI sont souvent importants et se doivent d'être gérés efficacement par l'entité, à défaut de quoi les risques inhérents pourraient augmenter (complexité plus grande et coûts généraux plus élevés).

Importance de l'intégrité des données pour une bonne gestion de l'information

Une bonne connaissance de la gestion de l'information inclut l'intégrité des données. Par intégrité des données, on entend l'exactitude, la validité et l'intégralité des données eu égard à leur utilisation prévue. Pour une entité, si les données ne sont pas intègres, sa tenue des documents, ses rapports et sa prise de décisions opérationnelles touchant les activités perdront en qualité. Pour l'auditeur, le niveau d'intégrité des données influencera le degré de confiance qu'il accordera aux données et à l'information pour planifier et exécuter son audit, communiquer les constatations et formuler des recommandations. L'intégrité des données est donc un élément déterminant de leur valeur et de leur utilité.

Normes régissant l'intégrité des données

Il existe plusieurs sources de normes régissant l'intégrité des données.

Le Manuel de CPA Canada — Certification, par exemple, exige que les praticiens tiennent compte de ce qui suit pour déterminer si les données sont fiables lorsqu'ils conçoivent leurs procédures analytiques de corroboration[2] :

- la source des informations disponibles (p. ex. sources indépendantes);
- la comparabilité des informations à celles de secteurs semblables;

[2] Manuel de CPA Canada — Certification : Normes canadiennes d'audit, chapitre 520, paragraphe A12.

- la nature et la pertinence des informations disponibles (à savoir, par exemple, si les budgets ont été établis en fonction des résultats attendus plutôt que des buts visés);
- les contrôles sur la préparation des informations sont conçus pour en assurer l'exhaustivité, l'exactitude et la validité.

En vertu du *Cadre stratégique pour l'information et la technologie* du Conseil du Trésor, les entités doivent assurer la confidentialité, l'intégrité et la disponibilité de l'information qui est essentielle à la prise de décisions et à la prestation des services du gouvernement.

Évaluation de l'intégrité des données

Dans le présent Guide, nous ne détaillons pas les caractéristiques de l'intégrité des données (p. ex. la validité, la vérifiabilité, la neutralité et l'exhaustivité). Cependant, l'équipe d'audit devrait, à l'étape de la planification, évaluer l'intégrité des données de l'information sur laquelle elle souhaite fonder ses constatations et ses conclusions d'audit de performance. Pour évaluer l'intégrité des données, l'auditeur pourra examiner les sources des données, telles que les fichiers de données (p. ex. l'inventaire des immobilisations corporelles), les opérations financières, les données sur l'Internet, les données de rapports sommaires, les extraits de données des bases de données ou des logiciels, et les rapports sur le rendement des programmes.

Les conditions suivantes pourraient conduire à la conclusion que l'intégrité des données est élevée :

- Le système ou le processus a été conçu par des personnes qui comprennent bien ce qu'est l'intégrité des données.
- L'intégrité des données est très importante pour les utilisateurs des rapports.
- L'information doit servir à rendre compte à des parties externes de haut niveau.
- Il est clair que l'entité changerait ses méthodes et ses procédures advenant un problème.
- L'entité a fait un échantillonnage des données en s'appuyant sur des principes rigoureux.
- Les données ont été bien gérées, et ce, de manière constante au cours des dernières années.
- Les données viennent d'un produit commercial établi (p. ex. PeopleSoft) et d'une fonction de production de rapports standard intégrée à ce produit.
- Le personnel de l'entité est conscient de la nécessité de l'intégrité des données et de son importance pour la prise des décisions cruciales, et a de l'expérience en la matière.
- Il est clair que les procédures et les contrôles relatifs à l'assurance de l'intégrité des données sont adéquats.
- Les données et les rapports sont soumis à l'examen et à l'approbation des décideurs, qui posent des questions liées à l'assurance de l'intégrité des données.
- Il existe des déclarations signées qui attestent de l'intégrité des données à partir d'analyses critiques documentées de l'interne ou de l'externe.

PLANIFICATION DE L'AUDIT

Aspects de la GI/TI relatifs au sujet de l'audit

Lors de la planification d'un audit de performance d'un programme ou d'un secteur, l'équipe d'audit devrait relever tout aspect relatif à la GI/TI susceptible de devenir un secteur d'examen. Par le passé, les secteurs d'examen d'un audit de performance liés à la GI/TI étaient plutôt traités séparément et n'étaient pas inscrits en complément dans l'ensemble des secteurs d'examen relatifs à un programme ou à un secteur. On supposait ainsi que les opérations des programmes et les composantes de la GI/TI étaient deux choses distinctes, qui devaient donc être auditées séparément. Maintenant, devant la place dominante que prend la GI/TI dans les opérations et vu que l'information est une ressource clé pour les audits de performance, les auditeurs devraient s'intéresser aux aspects de la GI/TI dans chaque audit.

Lors d'un audit de performance, le Bureau établit les secteurs d'examen à auditer en utilisant une approche fondée sur le risque qui suit les risques inscrits dans les plans stratégiques d'audit. Cela inclut les aspects de la GI/TI. Par conséquent, les secteurs d'examen relatifs à la GI/TI devraient faire partie de l'ensemble des secteurs d'examen. L'**annexe 1** donne des exemples de secteurs d'examen tirés de chapitres d'audits récents pour lesquels les auditeurs ont utilisé cette approche intégrée.

Questions à poser à l'étape de la planification et de l'établissement de l'étendue de l'audit

Au moment de planifier l'audit d'un programme ou d'un secteur et d'en établir l'étendue, l'équipe d'audit devrait tenter de répondre aux trois questions cruciales portant sur la GI/TI.

1. Quelles données appuient la capacité de la direction de prendre des décisions éclairées?
2. Ces données sont-elles fiables?
3. Le cadre de la GI/TI lié au programme ou au secteur concorde-t-il avec les objectifs opérationnels?

L'examen de ces facteurs aidera l'auditeur à déterminer si l'entité satisfait aux exigences du Conseil du Trésor en ce qui a trait à la gestion efficace de l'information, à savoir posséder :

- des structures, des mécanismes et des ressources de gouvernance adéquats;
- un accès pratique à de l'information pertinente, fiable, exhaustive et actuelle pour les programmes et les services gouvernementaux;
- des ressources appuyant les résultats des programmes et des services ainsi que les besoins opérationnels et les obligations de rendre compte.

Si l'auditeur juge que d'autres aspects de la GI/TI devraient être examinés, il y a un risque que l'audit de performance soit apparenté à un audit technique de la GI/TI. Il y aurait alors lieu de consulter la personne-ressource de l'équipe de la prestation des services et des technologies de l'information. Voir à cette fin la section Spécialistes internes de notre site INTRAnet, sous TI — Audit de performance.

Risques liés à la GI/TI

Les sujets de nos audits de performance sont choisis en fonction de l'évaluation des risques qui conduit aux plans stratégiques d'audit (PSA). À l'étape de la planification de son audit, l'auditeur fait un suivi en ajoutant continuellement des renseignements sur les opérations et en revoyant les résultats du PSA. Il s'entretient avec les représentants de l'entité et effectue des cheminements structurés pour confirmer la mesure dans laquelle ces risques sont actuels.

Pour les risques relatifs à la GI/TI cernés au départ dans le PSA et liés au programme ou au secteur audité, l'équipe d'audit devrait commencer par examiner le plan des risques d'entreprise (ou un document équivalent). Ce document devrait normalement montrer les risques relatifs à la GI/TI, classés par degré de gravité en fonction de leur impact et de la probabilité qu'un incident se produise. Les responsabilités et l'échéancier établis pour contrôler chaque risque devraient y être notés.

Les principales lignes directrices du Conseil du Trésor sur la gestion du risque d'entreprise sont contenues dans le Cadre stratégique de gestion du risque et le Guide de gestion intégrée du risque. L'étendue de l'audit de la GI/TI est influencée par les politiques du Conseil du Trésor énumérées ci-dessous. Voir aussi les normes et les directives rattachées à ces politiques.

- **Cadre stratégique pour l'information et la technologie**
- **Politique sur la gestion de l'information**
- **Politique sur la gestion des technologies de l'information**
- **Politique sur la sécurité du gouvernement**

Indicateurs de risques potentiels liés à la GI/TI

Les indicateurs de risques potentiels liés à la GI/TI, par domaine de gestion, que doit rechercher l'auditeur lorsqu'il établit l'étendue d'un audit de performance sont décrits ci-dessous. La liste d'exemples donnés n'est pas inclusive.

L'auditeur ne doit pas perdre de vue que s'il découvre un ou plusieurs de ces risques, il n'a pas à les inclure automatiquement dans son audit. Des contrôles compensatoires pourraient en minimiser la gravité. Le jugement professionnel est donc de mise au moment d'évaluer la mesure dans laquelle ces risques devraient être pris en compte dans l'étendue de l'audit.

Gouvernance

- Le dirigeant principal de l'information (DPI) ou son équivalent ne fait pas partie de l'équipe de la haute direction participant au processus décisionnel.
- Le DPI ou son équivalent se rapporte à un cadre hiérarchique (le directeur de la comptabilité par exemple) plutôt qu'à un haut dirigeant. Le cadre hiérarchique ne contrôle pas directement une section ou une direction générale qui est servie par le DPI.
- Il n'y a pas de planification opérationnelle ou stratégique en TI.
- Le plan stratégique d'entreprise ne comporte pas d'objectifs opérationnels liés à la GI/TI.

- Il n’y a pas de paramètres de mesure du rendement ou de carte de pointage pour suivre l’évolution des plans opérationnels ou tactiques en TI.
- Il n’y a pas de cadre en place pour évaluer les technologies nouvelles ou naissantes qui pourraient améliorer et transformer les opérations de l’entité.
- Il n’y a pas de planification relative aux risques liés à la TI (comme un cadre de gestion des risques liés à la TI) ou cette planification est inadéquate.
- Les risques liés à la GI/TI ne sont pas inclus dans les risques de l’entité.
- La fonction de vérification interne n’a ni revu ni examiné les secteurs de risques de la GI/TI depuis plusieurs années.
- Les secteurs clés, tels que celui du DPI et celui de l’agent de sécurité principal, connaissent un taux de roulement élevé dans les rangs de la direction et du personnel ou comptent des postes laissés vacants pendant de longues périodes.
- Pour la direction, la TI est un service entièrement dédié aux secteurs des activités, qui est privé de toute autorité pour remettre en question les exigences opérationnelles.
- Le nombre des personnes, en particulier à la comptabilité et aux systèmes de la TI, possédant les compétences requises compte tenu de la taille et de la complexité des opérations est inadéquat.
- Dans un audit sectoriel, plusieurs entités produisent de l’information commune servant à la prise de décisions, qui donne des résultats différents et pour laquelle il n’y a pour ainsi dire aucun rôle défini quant à la propriété des données.

Acquisition, développement et mise en œuvre de systèmes

Il n’y a pas de cadre de gestion de programme comprenant :

- un cycle de vie de projet;
- un cycle de contrôle de projet;
- des outils ou des gabarits facilitant l’exécution des projets.

Il n’y a pas de critères pour établir l’ordre de priorité des projets.

On sait que des projets axés sur la TI n’ont pas été réalisés dans les limites de budget et de temps établies au départ et que certains projets n’ont pas livré les fonctions attendues.

Les systèmes de comptabilité ou les systèmes d’information, y compris les systèmes de la TI, ne sont pas modifiés lorsque les conditions changent.

Opérations de la GI/TI

Les instruments suivants sont inexistants ou inadéquats :

- politique sur la sécurité de la TI;
- évaluation de la menace et des risques;
- plan de sauvegarde hors site;
- politique sur la continuité des activités;
- analyse des répercussions sur les activités;
- plan de reprise après sinistre pour les données et systèmes essentiels.

Les systèmes essentiels sont toujours compromis peu après une cyberattaque.

Prestation des services en GI/TI

Les données ou les instruments suivants sont inexistants ou inadéquats :

- ententes avec les clients ou ententes sur les niveaux de service;
- paramètres de mesure du rendement dans les ententes avec les clients ou les ententes sur les niveaux de service;
- justifications de la décision de recourir à l'impartition;
- surveillance des paramètres de mesure du rendement de l'impartition;
- politique de classement des documents électroniques.

Les principaux utilisateurs opérationnels critiquent la qualité de l'information servant à la prise des décisions cruciales.

Il n'y a pour ainsi dire aucune assurance que l'entité se conforme à toutes les lois en vigueur ou même à ses propres règles administratives.

Questions à examiner en rapport avec l'inclusion des données dans l'étendue de l'audit

Les données occupent une large place dans la gestion de l'information (GI). Les questions suivantes aideront à faire le lien entre la planification de la GI et l'établissement de l'étendue de l'audit. L'auditeur pourra s'en servir pour établir l'étendue de son audit et sélectionner les secteurs d'examen.

- Les données répondent-elles aux objectifs de sécurité suivants qui sont exposés dans la **Politique sur la sécurité du gouvernement** du Conseil du Trésor?

  Confidentialité : Les données assurent-elles la préservation des restrictions quant à l'autorisation d'accès?

  Intégrité : Les données sont-elles à l'abri d'une modification ou d'une destruction d'information inappropriée?

  Disponibilité : Les données assurent-elles une mise à disposition et une utilisation rapide et fiable de l'information?

- Les données sont-elles complètes et actuelles? Autrement dit, existe-t-il un cadre qui définit et maintient les responsabilités quant à la propriété de l'information ou des données, et des systèmes d'information correspondants? Y a-t-il des procédures protégeant l'intégrité et la cohérence des principales informations en format électronique (bases de données, entrepôts de données, archives)?
- Les données répondent-elles aux besoins de la majorité des utilisateurs opérationnels?
- Les données concordent-elles avec les buts et objectifs de l'entité?

À l'étape de la planification d'un audit de performance, l'équipe d'audit, par des entretiens et des cheminements structurés des opérations, devrait inclure dans l'étendue l'information et les systèmes des TI à examiner.

De là, les questions et les secteurs d'examen sont conçus pour la grille logique d'audit dont il est question dans la section suivante.

Questions de la grille logique d'audit

À l'étape de la planification de l'audit, les questions d'audit liées à la GI/TI sont élaborées. Ces questions deviennent les sous-critères à l'appui des principaux critères d'audit des activités du programme ou du secteur.

L'**annexe 2** contient des exemples de questions d'audit liées à la GT/TI qui viennent compléter l'audit de performance d'un programme ou d'un secteur, ainsi que des documents utiles à examiner à la lumière des trois questions cruciales exposées ci-haut dans la section intitulée « Questions à poser à l'étape de la planification et de l'établissement de l'étendue de l'audit ».

Documents et techniques utiles pour auditer la gestion de l'information

L'**annexe 3** donne des exemples de documents trouvés à l'intérieur et à l'extérieur de l'entité, qui sont utiles pour auditer la GI/TI.

POUR PLUS D'INFORMATION ET DE DIRECTIVES

Le présent Guide a été préparé par l'équipe de la prestation des services et des technologies de l'information. Pour plus d'information, consultez la personne-ressource de l'équipe dont les coordonnées se trouvent dans la section Spécialistes internes de notre site INTRAnet, sous TI — Audit de performance.

Si l'équipe d'audit repère des aspects de la GI/TI au moment de planifier son audit de performance, elle devrait consulter l'équipe de la prestation des services et des technologies de l'information (PSTI). Si elle songe à exclure des risques liés à la GI/TI importants de l'étendue de son audit, elle devra en évaluer l'impact en s'appuyant sur son jugement professionnel. Elle devrait, à tout le moins, consulter l'équipe de PSTI tôt à l'étape de la planification pour déterminer dans quelle mesure cette dernière devrait intervenir dans l'audit.

Tous les audits de performance sont différents lorsqu'il s'agit de l'intervention de l'équipe de PSTI. Cependant, cette intervention dépend en grande partie des facteurs suivants :

- impact de l'information diffusée au public (p. ex. reportages au sujet d'une attaque par refus de service lorsque les systèmes essentiels de l'entité examinés ne sont pas disponibles pendant une période prolongée);
- taille et complexité de l'audit;
- perception, par l'équipe d'audit, de la gravité des risques de la GI/TI à auditer;

- étendue planifiée de l’audit de la GI/TI (p. ex. nombre de modules de la GI/TI en cause, comme le plan de continuité des activités, la sécurité informatique et la planification stratégique des TI);
- expérience de l’équipe d’audit en ce qui a trait aux audits de performance de la GI/TI.

ANNEXE 1

EXEMPLES DE SECTEURS D'EXAMEN INTÉGRANT LA GI/TI

Les exemples de secteurs d'examen suivants (de même que leurs critères et objectifs d'audit) sont tirés de récents audits de performance dans lesquels la gestion de l'information et la technologie de l'information sont intégrées dans l'audit.

Des critères utilisés dans le *Rapport du vérificateur général du Canada* (printemps 2013), chapitre 7, « Les activités fédérales de recherche et sauvetage » (SAR) :

> « Les systèmes d'information SAR répondent adéquatement aux exigences opérationnelles, sont gérés correctement, et sont disponibles et utilisables quand il le faut. »
>
> « Les systèmes d'information SAR procurent des informations de qualité, répondent aux exigences stratégiques et facilitent les processus décisionnels et l'établissement de rapports. »

Des critères utilisés dans le *Rapport du vérificateur général du Canada* (automne 2013), chapitre 5, « Prévenir l'entrée illégale au Canada » :

> « Il existe des systèmes d'information essentiels à la prévention de l'entrée illégale de personnes au Canada qui :
>
> - fournissent une information de qualité;
> - sont disponibles et utilisables au moment voulu;
> - sont bien gérés;
> - facilitent la production de rapports ainsi que la prise de décision. »

ANNEXE 2

EXEMPLES DE QUESTIONS D'AUDIT LIÉES À LA GI/TI

Voici des exemples de questions d'audit liées à la GI/TI que peut poser une équipe d'audit pour l'audit de performance d'un programme ou d'un secteur, et des exemples de documents qu'elle peut examiner, guidée par les trois questions essentielles à poser à la planification et à l'établissement de l'étendue d'un audit de la GI/TI dont il est fait mention dans la section intitulée « Questions de la grille logique d'audit ».

Question de planification et d'établissement de l'étendue liée à la GI/TI	Questions d'audit liées à la GI/TI	Exemples de documents à examiner
1. Quelles sont les données disponibles?	• Quelles sont les principales données à auditer pour le programme et le secteur et quels sont les mécanismes et les structures de gouvernance en jeu? • Dans quelle mesure les utilisateurs opérationnels interviennent-ils dans le cadre d'évaluation des risques? • Comment l'entité s'assure-t-elle que les données permettent à la haute direction de prendre des décisions qui concordent avec la mission et le mandat?	• Organigramme de l'entité • Mandats et comptes rendus des groupes de travail et des comités principaux • Description générale du cadre d'évaluation des risques de l'entité • Rapports de vérification interne et évaluations de tiers • Description et avancement des projets axés sur la TI

Question de planification et d'établissement de l'étendue liée à la GI/TI	Questions d'audit liées à la GI/TI	Exemples de documents à examiner

2. Les données sont-elles fiables?	• Dans quelle mesure les données répondent-elles aux objectifs généraux de confidentialité, de disponibilité et d'intégrité liés à la sécurité?
	• Comment l'entité s'assure-t-elle que la sécurité de ses données se conforme à ses politiques internes et à la Politique sur la sécurité du gouvernement de même qu'aux autres politiques imposées de l'extérieur?
	• La réalisation des objectifs de sécurité a-t-elle déjà été jugée problématique? Le cas échéant, quelles mesures ont été prises?
	• Les responsabilités relatives à la propriété des données et à la reddition de comptes sont-elles clairement définies?
	• La section de la TI et les principaux utilisateurs opérationnels ont-ils conclu des ententes sur les niveaux de service? Le cas échéant, ces ententes couvrent-elles :
	  • la disponibilité,
	  • la fiabilité,
	  • le rendement,
	  • la possibilité de croissance,
	  • les niveaux de soutien pour les utilisateurs,
	  • la sécurité et la planification de la continuité?
		• Description et avancement des projets axés sur la TI
		• Évaluation de la menace et des risques
		• Rapports de vérification interne et évaluations de tiers
		• Autres documents internes montrant que l'entité se conforme à des politiques précises en matière de sécurité
		• Politique sur la sécurité
		• Politique sur l'intégrité des données
		• Mandats des groupes de travail sur l'intégrité des données
		• Cadres d'assurance de l'intégralité et de l'actualité des données
		• Exemples d'ententes sur les niveaux de services et de dispositions connexes

Question de planification et d'établissement de l'étendue liée à la GI/TI	Questions d'audit liées à la GI/TI	Exemples de documents à examiner
3. Le cadre de la GI/TI concorde-t-il avec les objectifs opérationnels?	• Avec quels mécanismes de rétroaction vérifie-t-on si les besoins en données des utilisateurs opérationnels sont satisfaits, et ce, de manière adéquate? • Le cadre de gouvernance garantit-il que les besoins des utilisateurs opérationnels sont satisfaits? • Le cadre de planification stratégique garantit-il que les besoins des utilisateurs opérationnels sont satisfaits? • Les documents stratégiques de l'entité tiennent-ils compte des données jugées nécessaires et de la stratégie en la matière?	• Résultats des enquêtes internes sur les besoins des utilisateurs opérationnels et plans d'action connexes dans lesquels sont exposés les problèmes et les mesures prises pour les régler. • Description du cadre de gouvernance en rapport avec la pertinence des données requises pour la prise des décisions de gestion cruciales. • Plan stratégique • Plan opérationnel (ou tactique) • Rapports de vérification interne et évaluations de tiers

ANNEXE 3

EXEMPLES DE DOCUMENTS UTILES POUR AUDITER LA GI/TI

Documents internes

- Plans stratégique et opérationnel de la GI/TI
- Plans d'investissement en GI/TI
- Cadres de mesure du rendement en GI/TI
- Plan de continuité des activités et autres plans connexes
- Politiques (p. ex. sécurité informatique)
- Comptes rendus des comités de gestion principaux qui influencent les décisions importantes en GI/TI et présentations et notes d'information connexes
- Relevé des risques de l'entité (ou document équivalent) montrant les risques liés à la GI/TI
- Évaluation des risques liés à la GI/TI (si elle ne fait pas partie du relevé des risques de l'entité)
- Rapports de vérification interne et études de tiers visant la GI/TI
- Présentations au Conseil du Trésor et mémoires au Cabinet touchant les décisions importantes en GI/TI

Documents accessibles en ligne

- Articles récemment publiés dans les médias, revues spécialisées
- Mises à jour parlementaires
- Comptes publics : informations détaillées (p. ex. systèmes de la GI/TI vieillissants, les « anciens » systèmes)
- Rapports des comités du Sénat et de la Chambre des communes touchant les décisions importantes en GI/TI

Techniques d'audit (communes à tous les audits de performance)

- Entretiens
- Analyse de documents
- Technique du cheminement structuré, une technique d'audit comportant un entretien avec les représentants de l'entité pour aider l'équipe d'audit à mieux comprendre les cadres relatifs à :

    - la planification stratégique et opérationnelle;
    - l'évaluation des risques, leur priorisation et les mesures d'atténuation;
    - la gestion du programme d'investissement (y compris les projets axés sur la GI/TI);
    - l'assurance de l'intégrité des données.

- Consultation auprès de l'équipe de la prestation des services et des technologies de l'information au début de l'étape de la planification