**Guide d’évaluation des risques liés à l’examen spécial
des systèmes de technologies de l’information**

**Table Des Matière**

Technologies De L’information 3

La démarche proposée repose sur la méthode d’examen spécial du Bureau du vérificateur général du Canada : 3

Critères et sous-critères de vérification liés aux TI 4

Évaluation des risques : 5

Annexe – Liste des documents demandés pour l’évaluation des risques liés à l’examen spécial des technologies de l’information (TI) 17

|  |
| --- |
| Technologies De L’informationLa démarche proposée repose sur la méthode d’examen spécial du Bureau du vérificateur général du Canada :Le présent guide d’évaluation des risques a pour but d’aider le vérificateur à évaluer les risques liés aux systèmes de technologies de l’information (TI) et aux pratiques au cours de la phase de planification d’un examen spécial. À la fin de la présente évaluation, le vérificateur sera en mesure de déterminer si les risques liés aux technologies de l’information peuvent avoir une incidence sur l’atteinte d**es objectifs de contrôle législatif de** la société d’État.Ce guide est conforme aux pratiques exemplaires dans le domaine de la vérification des technologies de l’information telles que décrites dans CobiT 4.0, ISO 17799, ITIL, Val IT et le 2007 Certified Information Systems Auditor (CISA) Review Manual. Le guide d’évaluation a été rédigé sous forme condensée et compte tenu de la nature spécialisée du sujet et de la complexité de l’environnement des TI, des travaux supplémentaires peuvent s’avérer nécessaires. Dans ce cas, il est recommandé de consulter l’expert interne de la vérification de gestion des technologies de l’information.Avant de procéder à l’évaluation des risques, le vérificateur devrait acquérir une compréhension globale des activités de l’entité. Il peut à cette fin examiner des documents comme le plan d’entreprise. Afin d’éviter le chevauchement des efforts, il devrait consulter les renseignements contenus dans les dossiers d’attestation, plus précisément la section C.8 du plus récent dossier TeamMate de l’entité.La prochaine étape consiste notamment à prévoir une première réunion avec le responsable des systèmes de technologies de l’information de l’entité, qui est habituellement le dirigeant principal de l’information (DPI). À cette réunion, le vérificateur apporte la liste de documents qu’il désire obtenir de son client et s’assure que ce dernier a bien compris ce qu’on lui demande (voir l’Annexe). Il détermine quelles sont les personnes clés à rencontrer aux différentes étapes des quatre sections du présent guide d’évaluation des risques.Après avoir rempli le questionnaire d’évaluation des risques et examiné les documents obtenus, le vérificateur devrait rédiger un court rapport dressant la liste des secteurs d’examen possibles et des constatations qui pourraient empêcher l’entité d’atteindre les résultats escomptés. Le rapport devrait décrire la méthode de collecte des éléments probants et indiquer les ressources et le temps qui seront nécessaires pour réaliser la phase d’examen.Si des secteurs d’examen particuliers ont été approuvés pour la phase d’examen, des programmes de vérification supplémentaires devront être conçus (p. ex. planification stratégique des TI, gestion des projets en matière de TI, sécurité des TI, prestation de services de TI). |

## Critères et sous-critères de vérification liés aux TI

|  |
| --- |
| La planification, la mise au point, la mise en œuvre et la gestion des technologies de l’information et des systèmes d’information appuient les objectifs stratégiques et opérationnels de l’organisme, assurent la continuité de ses activités et répondent aux besoins en information, à un coût acceptable et en temps voulu.  |
| 1. Les plans stratégiques et opérationnels en matière de technologies de l’information sont harmonisés avec l’orientation et les priorités de la société et ils les appuient. Ces plans devraient être réévalués périodiquement et modifiés en fonction de l’évolution des activités et des conditions des TI.
2. L’acquisition de systèmes informatiques tient compte des besoins à la fois des utilisateurs et de l’ensemble de la société, ainsi que des risques cernés et des seuils de tolérance connexes.
3. Les systèmes d’information sont disponibles et utilisables au besoin. Ils sont conçus pour résister aux attaques et assurer la reprise des activités après une panne.
4. Les activités liées à la gestion de l’information et aux technologies de l’information (GI‑TI) permettent d’offrir un service à la clientèle de qualité tout en veillant à l’efficience et à l’efficacité des processus et des activités.
 |

**TECHNOLOGIES DE L’INFORMATION**

## Évaluation des risques :

| Étape | Description | Par | Document de référence |
| --- | --- | --- | --- |
| **1 Les plans stratégiques et opérationnels en matière de technologies de l’information sont harmonisés avec l’orientation et les priorités de la société et ils les appuient. Ces plans devraient être réévalués périodiquement et modifiés en fonction de l’évolution des activités et des conditions des TI.** |
| 1.1 | Se reporter à la liste de documents et examiner ceux qui sont mentionnés dans la présente section.1. Pour l’examen du plan stratégique des TI, prendre en compte ce qui suit :
	1. Le plan contient un aperçu de la vision de l’Unité des TI; les objectifs stratégiques en matière de TI sont liés aux objectifs organisationnels; les projets ont des échéanciers et leurs avantages sont précisés; les nouvelles technologies ont fait l’objet d’un examen; les indicateurs de rendement et les ressources sont inclus.
	2. Le plan est harmonisé avec les risques d’entreprise et en matière de TI.
2. Pour l’examen des plans tactiques et opérationnels en matière de TI, prendre en compte ce qui suit :
	1. Les plans présentent des objectifs précis, les responsabilités, les mesures à prendre, les échéanciers et les ressources.
	2. Les plans et les tâches sont compris et acceptés l’entreprise et les TI.
 |  |  |
| 1.2 | Acquérir une compréhension de l’environnement de gouvernance  au moyen de discussions avec les cadres supérieurs des TI,:1. Le secteur des TI est‑il représenté au sein des principaux comités de direction? Comment est‑il représenté?
2. Quelles questions liées aux TI font l’objet de discussions à ces réunions?
3. Au sein de quels autres comités le secteur des TI est‑il représenté? (comités directeurs, comités d’utilisateurs)
 |  |  |
| 1.3 | Acquérir une compréhension de l’efficience et de l’efficacité des processus de planification annuels et stratégiques en matière de TI au moyen de discussions avec les cadres supérieurs des TI,. Prendre en compte ce qui suit :1. Les cadres supérieurs des TI comprennent-ils bien les plans des utilisateurs et des TI? Comprennent-ils en quoi les plans des TI appuient les plans d’entreprise?
2. Les cadres supérieurs des TI collaborent‑ils avec les autres gestionnaires des TI à l’élaboration des plans en matière de TI?
3. Comment procède‑t‑on pour demander aux parties prenantes ou aux partenaires internes et externes visés de prendre part à l’élaboration du plan stratégique en matière de TI?
4. Comment l’information utilisée au cours du processus décisionnel est-elle validée?
5. Qui approuve le plan stratégique des TI et quand cette personne l’approuve‑t‑elle?
6. Comment les éléments du plan stratégique des TI sont‑ils intégrés aux plans tactiques/opérationnels?
7. Des processus ont‑ils été mis en place en ce qui concerne les changements qui sont apportés au plan? Sont‑ils suivis?
 |  |  |
| 1.4 | Au moyen de discussions avec les cadres supérieurs des TI, acquérir une compréhension du processus d’intégration des nouvelles technologies à l’environnement TI actuel :1. Les possibilités en matière de TI et les nouvelles technologies de l’information sont‑elles des éléments importants du plan stratégique des TI?
2. Comment demande‑t‑­on de l’information sur l’utilisation des nouvelles technologies? Comment est‑elle reçue?
3. Comment détermine‑t‑on les avantages des nouvelles technologies? (p. ex. les avantages éventuels sont‑ils évalués?)
 |  |  |
| 1.5 | Conclure par rapport au sous‑critère 1. |  |  |

| Étape | Description | Par | Document de référence |
| --- | --- | --- | --- |
| **2 L’acquisition de systèmes informatiques tient compte des besoins à la fois des utilisateurs et de l’ensemble de la société, ainsi que des risques recensés et des seuils de tolérance qui s’y rattachent.**  |
| 2.1 | Se reporter à la liste de documents et examiner ceux qui sont mentionnés dans la présente section.Pour l’examen des documents et les discussions avec la direction des TI, prendre en compte ce qui suit :Note : En l’absence d’une méthode officielle, poser les questions ci‑dessous sur les procédures et les processus qui devraient être en place.1. Y a‑t‑il un énoncé de projet (aperçu) qui indique en quoi le projet correspond à l’orientation stratégique et aux plans de l’entité?
2. Est‑il requis de créer les documents suivants : (analyse de rentabilisation, charte du projet, plan du projet, registre des risques)?
3. Ces documents clés du projet doivent‑ils correspondre aux besoins des utilisateurs et aux plans de gestion de l’information?
4. Les structures de projet doivent‑elles définir les principales responsabilités, notamment en ce qui concerne le parrainage, les comités directeurs et la direction?
5. La répartition des responsabilités, la répartition des tâches, le temps et les ressources prévus, les étapes clés, les points de vérification et les approbations sont‑ils au moins couverts?
6. Les gestionnaires de projet appliquent‑ils la même méthode de gestion de projet de façon uniforme?
7. Est‑il facile d’adapter la méthode de gestion de projet aux différents types et tailles de projets?
8. La vérification interne collabore‑t‑elle aux projets de TI et, dans l’affirmative, de quelle manière?
 |  |  |
| 2.2 | Au moyen de discussions avec le directeur des TI et de l’examen des rapports de surveillance, acquérir une compréhension des processus de maintenance et de surveillance des systèmes des TI. Prendre en compte ce qui suit :1. Comment les rapports sur le rendement servent‑ils à atteindre les objectifs de la direction?
2. Existe‑t‑il un processus approprié pour la saisie, l’enregistrement, le règlement et le suivi des problèmes signalés?
3. Utilise‑t‑on des mécanismes de suivi pour les demandes de changement, les approbations, les priorités, les affectations et l’acceptation par les utilisateurs?
4. En ce qui concerne les principaux changements apportés à la maintenance, dresse‑t‑on un bilan pour déterminer si les avantages prévus ont été obtenus et s’ils sont conformes aux plans de l’organisme.
5. Les coûts réels et les produits à livrer sont‑ils comparés aux estimations initiales?
 |  |  |
| 2.3 | Pour l’examen du portefeuille du projet et les discussions avec le directeur des TI, prendre en compte ce qui suit :1. Existe‑t‑il des politiques organisationnelles qui décrivent comment l’ordre de priorité des projets est établi et les ressources sont affectées?
2. Dans quelle mesure les analyses coûts‑avantages sont‑elles utilisées pour établir l’ordre de priorité des projets et pour les approuver?
3. Le processus d’établissement des priorités exige‑t‑il que les projets à l’étude soient liés aux besoins et aux plans des utilisateurs?
4. Qui décide à quels projets les ressources seront affectées?
5. Comment s’assure‑t‑on qu’il y a suffisamment de ressources adéquates pour le nombre de projets acceptés?
6. Comment s’assure‑t‑on d’obtenir les ressources requises pour les projets internes des TI?
7. Comment l’ordre de priorité des projets est‑il modifié?
 |  |  |
| 2.4 | Au moyen de discussions avec les cadres supérieurs des TI et de l’examen des documents pertinents, comme les politiques d’évaluation des risques et les comptes rendus de réunion, déterminer si les décisions de gestion des projets sont fondées sur la gestion des risques. Prendre en compte ce qui suit :1. Les grands projets complexes sont‑ils subdivisés en sous‑projets plus gérables et moins risqués?
2. Dans quelle mesure la direction coordonne‑t‑elle efficacement chacun des sous‑projets?
3. Des points de vérification ou des jalons d’approbation préétablis permettent‑ils un examen indépendant de sorte que la direction puisse prendre des décisions quant à l’avenir du projet ou à la prise de mesures correctives appropriées?
4. Revoit‑on le rendement du projet à chaque jalon d’approbation préétabli ou lorsque les fonds sont épuisés?
5. Évalue‑t‑on les risques et établit‑on les points de vérification et jalons d’approbation préétablis?
6. Tient‑t‑on des registres des risques et des journaux des risques pendant toute la durée du projet?
7. De quels outils et méthodes l’organisation dispose‑t­elle pour gérer les risques du projet?
 |  |  |
| 2.5 | Au moyen de discussions avec la direction des TI et de l’examen des documents connexes, acquérir une compréhension du cycle de développement des systèmes utilisé l’organisme. Prendre en compte ce qui suit, le cas échéant :1. Les utilisateurs des systèmes collaborent‑ils pleinement pour faire en sorte que les systèmes répondent à leurs exigences?
2. Quelles sont les responsabilités du groupe des technologies de l’information?
3. Le cycle de développement des systèmes comprend‑il l’évaluation des compétences requises par rapport aux compétences actuellement exigées?
4. Les clients et le groupe des TI participent‑ils aux examens aux jalons d’approbation préétablis du projet et aux décisions subséquentes touchant l’avenir du projet?
5. Existe‑t‑il des processus d’évaluation de l’incidence des changements apportés à l’étendue du projet?
 |  |  |
| 2.6 | Conclure par rapport au sous‑critère 2. |  |  |

| Étape | Description | Par | Document de référence |
| --- | --- | --- | --- |
| **3 Les systèmes d’information sont disponibles et mis en service lorsque cela est nécessaire. Ils sont conçus pour résister aux attaques et assurer la reprise des activités après une panne.** |
| 3.1 | Se reporter à la liste de documents et examiner ceux qui sont mentionnés dans la présente section.Examiner les politiques sur la sécurité des TI afin d’établir si elles touchent les secteurs suivants :1. Gestion des identités, gestion des comptes d’utilisateur, tests de sécurité, surveillance, définition d’incident de sécurité, protection des technologies de la sécurité, sécurité du réseau, prévention, détection et correction des logiciels malveillants.
2. Si un comité de sécurité est en place, examiner son mandat et les comptes rendus des réunions.
3. S’il n’y a pas de comité, demander comment les questions de sécurité sont communiquées à la direction.
 |  |  |
| 3.2 | Au moyen de discussions avec le directeur des TI et l’agent de sécurité, acquérir une compréhension du programme de sécurité de l’information et de sa gouvernance. Prendre en compte ce qui suit :1. L’organisme a‑t‑il approuvé la politique sur la sécurité des TI?
2. Quelles sont les normes mentionnées dans les politiques de sécurité de l’entité? (p. ex. ISO17799, politiques du gouvernement sur la sécurité)
3. Y a‑t‑il un programme de sensibilisation à la sécurité? Le personnel des TI et les autres employés sont‑ils informés au sujet des politiques et des lignes directrices en matière de sécurité?
4. Existe‑t‑il des rapports qui résument les résultats du programme de surveillance? Qui examine ces rapports? Les questions importantes sont‑elles transmises aux paliers supérieurs?
5. À quelle fréquence les cadres supérieurs prennent‑ils part à la recherche de solutions aux problèmes de sécurité et à l’approbation des solutions?
6. Les employés sauraient‑ils reconnaître un incident de sécurité s’il s’en produisait un?
7. A‑t‑on instauré un système de gestion des incidents? Dans la négative, l’organisme sait‑il s’il y a eu des tentatives d’attaque ou d’intrusion?
8. Comment les incidents sont‑ils observés et signalés et à qui sont‑ils signalés?
9. Y a‑t‑il des politiques pour s’assurer que l’information est accessible et communiquée uniquement aux personnes autorisées et qu’elle est protégée contre toute modification non autorisée?
10. Existe‑t‑­il des politiques et des procédures appropriées pour la garde des documents électroniques?
11. Comment l’organisme s’assure‑t‑il que ses systèmes sont conformes aux lois et aux règlements pertinents? (protection des renseignements personnels, droits d’auteur, etc.)
12. Comment l’entité a‑t‑elle atténué tous les risques pour les TI recensés?
 |  |  |
| 3.3 | Au moyen de discussions avec le directeur des TI, acquérir une compréhension du programme de la continuité des TI. Prendre en compte ce qui suit :1. Y a‑t‑il un plan de reprise après sinistre (PRS) en TI qui comprend les applications, les systèmes, les réseaux et les données?
2. Quand le plan de reprise après sinistre en TI a‑t‑il été testé la dernière fois?
3. Existe‑t‑il une liste des ressources essentielles en TI et sont‑elles classées selon un ordre de priorité aux fins de la reprise?
4. Les outils et les processus requis pour exécuter une sauvegarde fréquente des données et du logiciel d’exploitation sont‑ils en place?
5. Que prévoit le plan de la continuité (grave interruption et aucune ressource en TI disponible ou seulement interruption négligeable et toutes les ressources disponibles)?
6. Des objectifs pour le temps de reprise ont‑ils été établis pour tous les services et les secteurs fonctionnels de l’organisme?
7. A‑t‑on un processus documenté de transmission aux paliers supérieurs qui montre comment les plans de la continuité sont mis en oeuvre?
8. Une installation externe est‑elle prévue pour conserver les supports de sauvegarde essentiels? Comment ce site est‑il géré? Les sauvegardes de reprise ont‑elles été testées?
 |  |  |
| 3.4 | Conclure par rapport au sous‑critère 3. |  |  |

| Étape | Description | Par | Document de référence |
| --- | --- | --- | --- |
| **4 Les activités liées à la gestion et aux technologies de l’information permettent d’offrir un service de qualité à la clientèle tout en assurant l’efficience et l’efficacité des processus et des opérations.**  |
| 4.1 | Se reporter à la liste de documents et examiner ceux qui sont mentionnés dans la présente section. |  |  |
| 4.2 | Au moyen de discussions avec la direction des Systèmes d’information, acquérir une compréhension des pratiques utilisées pour assurer la qualité du service à la clientèle. Prendre en compte ce qui suit :1. Le niveau d’orientation (faire part des besoins) et de participation des utilisateurs des TI est‑il satisfaisant?
2. Les ententes de service officielles portent‑elles au moins sur les aspects suivants : disponibilité, fiabilité, rendement, capacité de croissance, niveaux de soutien requis pour les utilisateurs, planification de la continuité et sécurité?
3. Comment l’organisme s’y prend‑il pour surveiller le respect des critères de service spécifiés et les problèmes et faire rapport sur ceux‑ci?
4. Y a‑t‑il un programme d’amélioration du service pour réaliser les améliorations des niveaux de service dont les coûts ont été justifiés?
5. Existe‑t‑il un cadre et des processus pour garantir le respect des normes légales et réglementaires et d’autres normes? (analyse de sensibilité pour l’évaluation de la menace et des risques, gestion de licence, autorisation de sécurité).
 |  |  |
| 4.3 | Au moyen de discussions avec le directeur des TI et de la consultation des documents connexes, acquérir une compréhension des pratiques d’impartition de certains systèmes ou services de TI. Prendre en compte ce qui suit :1. Existe‑t‑il des méthodes et des procédures documentées pour sélectionner et gérer les tiers fournisseurs? Sont‑elles mises en application?
2. Les ententes contractuelles avec des tiers sont­‑elles examinées par les parties concernées?
3. Les ententes de niveau de service conclues avec des tiers sont‑elles claires? Comment surveille‑t‑on le rendement des tiers fournisseurs de services?
4. Les tiers sont‑ils tenus de respecter les normes de sécurité et de confidentialité?
5. Le groupe des TI ou la vérification interne font‑ils des vérifications appropriées des services fournis par les tiers?
 |  |  |
| 4.4 | Au moyen de l’examen des documents connexes, comme les contrats, et des discussions avec le gestionnaire de projet, acquérir une compréhension du processus de surveillance continue des services fournis par les tiers qui exécutent les projets de l’entité. Prendre en compte ce qui suit :1. Les tiers qui prennent part à l’élaboration ont‑ils une stratégie et des plans de transfert des connaissances aux ressources internes?
2. Est‑ce que le plan de transition garantit une maintenance appropriée des systèmes et des améliorations dans le futur?
3. A‑t‑on dressé des bilans et préparé des documents de clôture pour les sous‑projets ou des projets semblables?
 |  |  |
| 4.5 | Conclure par rapport au sous‑critère 4. |  |  |

# Annexe – Liste des documents demandés pour l’évaluation des risques liés à l’examen spécial des technologies de l’information (TI)

| **Documents** | **Réf.** | **Commentaires** |
| --- | --- | --- |
| 1 | Plan stratégique de TI | **1** |  |
| 2 | Budgets stratégiques et opérationnels (année en cours et pluriannuel) | **1, 2** |  |
| 3 | Structure de gouvernance des TI (principaux comités, mandat, et d’échantillonnage de comptes rendu de réunion) | **1** |  |
| 4 | Statistiques / mesures utilisées pour évaluer le rendement des services de TI | **1** |  |
| 5 | La dernière version de l’organigramme et des descriptions de tâches du personnel de niveau supérieur en TI  | **1** |  |
| 6 | Évaluation de la menace et des risques à l’échelle de l’organisation | **1** |  |
| 7 | Évaluation de la menace et des risques de TI | **1** |  |
| 8 | L’analyse de répercussions sur les activités (dans l’ensemble et/ou d’applications ou de systèmes individuels) | **3** |  |
| 9 | L’analyse des répercussions des lois et des règlements sur les processus de TI (c’est-à-dire sur la vie privée, le commerce électronique, la propriété intellectuelle…) - (dans l’ensemble et/ou d’applications ou de systèmes individuels) | **3.2** |  |
| 10 | L’évaluation de la vulnérabilité / rapports de tests de pénétration (dans l’ensemble et/ou d’applications ou de systèmes individuels) | **3** |  |
| 11 | Procédures de traitement des incidents de TI | **3** |  |
| 12 | Plan de continuité opérationnelle de l’organisation et la preuve de sa mise à jour | **3** |  |
| 13 | Résultats les plus récents de l’essai du plan de continuité opérationnelle | **3** |  |
| 14 | Le plan de reprise des TI après catastrophe / la preuve de sa mise à jour et les résultats les plus récents de l’essai du plan | **3** |  |
| 15 | Politiques et des procédures de TI liées au traitement des données électroniques, à leur classification et conservation | **3.2** |  |
| 16 | Politiques de sécurité / les outils de formation pour le programme de sensibilisation en matière de sécurité | **3** |  |
| 17 | Ordinogramme de réseau récent – vue d’ensemble | **4** |  |
| 18 | Inventaire des principales applications (essentielles à la mission de l’organisation) | **2, 3** |  |
| 19 | Méthodologie de développement de projets TI  | **2** |  |
| 20 | Contrats de TI (sous-traitance/impartition de services) Par exemple : hébergement web; fournisseur de services Internet; centre de soutien technique, commerce électronique, etc.  | **4** |  |