Gestion des risques liés à la Sécurité des TI au sein du gouvernement du Canada

JUILLET 2016 | SERIE HAUTS DIRIGEANTS | ITSE.10.033

Compte tenu du caractère dynamique de l'environnement de menace actuel et des contraintes financières du gouvernement du Canada (GC), la sécurité des technologies de l'information (TI) ne peut plus être reléguée au second plan et doit désormais être une composante essentielle des plans de projet TI et des ministères.

Les risques liés à la sécurité des TI peuvent mener à l'exposition d'information sensible du gouvernement, occasionner une perte de productivité, empêcher les ministères et organismes de remplir leurs objectifs ou porter atteinte à la réputation du GC. Tous ces risques peuvent coûter cher au GC.

La gestion des risques liés à la sécurité des TI est le processus par lequel les ministères et organismes gèrent les risques liés à la sécurité des TI grâce à la gestion et à l'application de contrôles, de solutions, d'outils et de techniques de sécurité conçus pour protéger les biens TI contre les compromissions.

Le cadre de gestion des risques liés à la sécurité des TI du CST peut aider à l'élaboration d'une stratégie de gestion des risques qui sera alignée sur l'affectation des ressources et les priorités du GC en vue de répondre aux objectifs des ministères.

Responsabilité du ministère

Le **responsable opérationnel** du système TI devrait mettre en œuvre les mesures ci-dessous lors de la prise de décisions sur la gestion des risques liés à la sécurité des TI.

- ✓ Déterminer le niveau de risque le plus élevé pouvant être toléré.
- ✓ Consulter les spécialistes de la planification de la continuité des activités, de la protection de la vie privée, de la gestion de l'information, et d'autres spécialistes fonctionnels pour veiller à ce que les risques dans ces domaines de responsabilité soient cernés et gérés.
- ✓ Formuler des décisions concernant les risques liés à la sécurité des TI à l'intention de l'agent de sécurité du ministère.
- ✓ Accorder l'**autorisation d'exploiter** après que les risques ont été cernés et atténués ou acceptés.
- ✓ Veiller à ce que les risques soient évalués de nouveau à la lumière des changements à la valeur des biens, aux menaces ou aux vulnérabilités afin de conserver l'autorisation d'exploiter les systèmes TI.

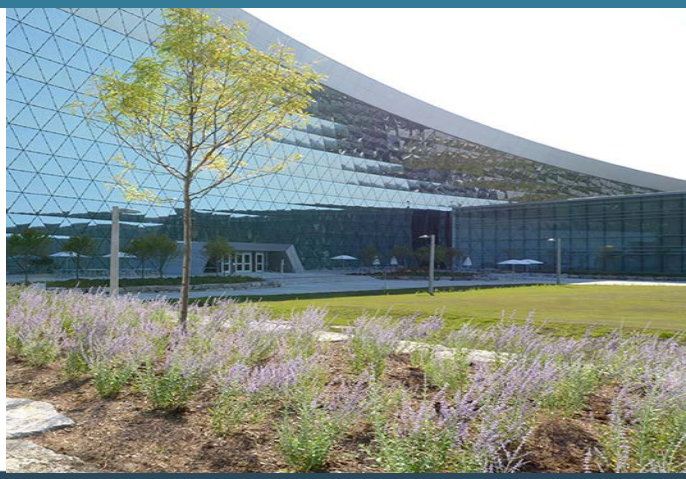
L'autorisation d'exploiter est l'approbation que le responsable opérationnel accorde à l'exploitation d'un projet ou d'un programme, d'une installation ou d'un système dont le fonctionnement est régi par un ensemble précis de mesures de sécurité et comporte un niveau de risque résiduel acceptable.

Bâtir et consolider

Comme la sécurité des TI est un processus itératif qui évolue selon le contexte de menace, les ministères devraient favoriser une approche de mise en œuvre de la sécurité des TI à la fois holistique et stratégique.

Les ministères doivent continuellement évaluer, planifier, créer et exécuter des programmes efficaces de sécurité des TI qui tiennent compte de la gestion des risques liés aux TI, de la gouvernance, des exigences opérationnelles et de la conformité.

La gestion des risques liés aux TI permet aux ministères de prendre des mesures à l'égard des risques liés aux lois, aux finances, à la conformité, à la réputation, aux politiques, aux opérations et à la vie privée.



Canada

Un instrument opérationnel

L'ITSG-33, La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie, du CST a été élaboré afin d'aider les ministères du GC à envisager dès le début les enjeux liés à la sécurité. L'ITSG-33 est une cadre permettant aux ministères d'évaluer et d'atténuer les risques par l'application efficace de contrôles de sécurité qui protègent l'information contre la compromission de la confidentialité, de l'intégrité et de la disponibilité. En appliquant les principes de l'ITSG-33, vous assurez non seulement la prévisibilité et la rentabilité, mais aussi la protection contre les mauvaises surprises qui pourraient vous empêcher d'obtenir et de conserver l'**autorisation d'exploiter** du responsable opérationnel du système TI.

Vous voulez en savoir plus?

Suivez le cours 604, *Survol de la gestion des risques liés à la sécurité des TI*, offert par Le Centre de formation en sécurité des TI du CST.

Selon la ***Norme de sécurité opérationnelle : Gestion de la sécurité des technologies de l'information*** du SCT, les gestionnaires de la prestation de programmes et de services doivent fournir un niveau de sécurité approprié pour leurs programmes et services.

Une approche intégrée

La gestion des risques liés à la sécurité des TI établit les rôles, les responsabilités et les activités qui aideront les ministères du GC à gérer les risques liés à la sécurité des TI. En suivant les stratégies de gestion des risques énoncées dans *l'ITSG-33, La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie*, *les ministères :*

- ✓ prennent en charge efficacement tous les aspects de la sécurité des TI;
- ✓ répondent aux besoins opérationnels de sécurité du ministère;
- ✓ améliorent la prise de décisions liées à la gestion des risques;
- ✓ respectent les politiques et les normes du GC.

Pour en savoir plus sur la gestion des risques liés à la sécurité des TI, consultez le site Web du CST :

www.cse-cst.gc.ca/fr/its

Questions?

Communiquez avec les Services à la clientèle de la STI à itsclientservices@cse-cst.gc.ca ou au 613-991-7654.

La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie

Le respect des lignes directrices énoncées dans l'ITSG-33 procure plusieurs avantages aux ministères, notamment la capacité de se conformer à la stratégie et aux objectifs de la gestion globale des risques établis par le SCT, de traiter de manière efficace les principaux aspects de la sécurité des TI et de gérer de manière uniforme et rentable les risques liés à la sécurité des TI.