Concours national d'essais universitaires

Les audits de cyber-sécurité au secours des organisations publiques

Eriole Zita Nonki Tadida
Étudiante en science politique

Université Laval, Québec

1500 mots

Novembre 2019

Introduction

La cyber-sécurité est un enjeu de défense nationale au Canada depuis la guerre froide, avec la création du Centre de Sécurité des Télécommunications (Loiseau *et coll.* 2013). Cependant, le développement des technologies de l'information (TI) et le virage numérique initié par le gouvernement depuis 2015 exposent les organisations publiques à de nouvelles menaces (Venne, 2019a). La modernisation des mécanismes de contrôle[1] est nécessaire, afin d'assurer la sécurité des informations sensibles gérées par ces organisations. L'audit interne peut y jouer un rôle essentiel, reconnu comme mécanisme contribuant à la bonne gestion des ressources publiques (Tremblay, 2011), qu'elles soient financières, matérielles ou informationnelles.

Bien qu'existant dans l'administration publique canadienne depuis les années 70 (Charko, 2013), l'audit interne semble encore un domaine méconnu. Pourtant il s'assure, par une approche méthodique et systématique, que les procédures, les systèmes de contrôle interne, de management des risques et de gouvernance concourent efficacement à la réalisation des objectifs de l'organisation (IIA, 2017). Or, la transformation numérique apporte des changements dans les systèmes des organisations : informations virtuelles et logiciels augmentent les risques de cyberattaques. Les auditeurs internes et les comités d'audits sont-ils outillés pour réaliser efficacement leur travail dans ce contexte? Que peut faire le gouvernement fédéral pour assurer cette efficacité?

L'audit interne a un rôle important dans cette époque de données massives. Le coût financier des pertes de données (près de 17 milliards$ au Canada[2]; environ 22000$/jour selon Henrard, 2019) devrait être réduit au minimum. Il n'est pas exagéré de dire, qu'au milieu des autres formes de contrôles, les audits de cyber-sécurité s'imposent.

Une courte présentation des transformations sociales liées au numérique précèdera la nécessité des audits de cyber-sécurité et la formation des auditeurs internes.

---

[1] Le gouvernement s'est engagé à adopter des approches modernes en matière de contrôle. Gouvernement du Canada, Suivi des lettres de mandat : livrer des résultats pour les canadiens. https://www.canada.ca/fr/conseil-prive/campagnes/mandat-suivi-resultats-canadiens.html , consulté le 18 octobre 2019. [2] Therrien Yves, Sécurité informatique : les pertes de données coutent plus de 16,8 milliards $ au Canada; publié le 3 décembre 2014, mis à jour le 3 février 2015. https://www.lesoleil.com/affaires/techno/securite-informatique-les-pertes-de-donneescoutent-168milliards--au-canada-4a1af7b9b60192d059cf1d7bde571322, consulté le 25 octobre 2019.

L'ère de la transformation numérique et les défis qui l'accompagnent

Le virage numérique fait partie des enjeux contemporains : dématérialisation, accès aux données, services en ligne, transparence sont quelques termes qui gouvernent ce changement. La délivrance des services aux citoyens y est immergée. Il s'agit par exemple d'utiliser son ordinateur ou son téléphone pour transmettre sa déclaration d'impôts, faire sa demande de passeport, prendre rendez-vous chez le médecin. La vie numérique impacte le quotidien des citoyens (Welby, 2019), mais aussi oblige une mutation dans les processus organisationnels : milliers de courriels échangés par jour, transmissions des documents sur différentes plateformes qui alimentent des prises de décisions. Afin d'assurer la fiabilité de ces informations, les organisations doivent s'équiper du matériel technologique adéquat, mais surtout revoir leurs procédures, systèmes de contrôle interne et gestion des risques (Nikoloyuk *et coll*. 2005). Car, si la transformation numérique démontre ses bénéfices en termes d'accessibilité aux données ou de gain temporel, elle apporte aussi plusieurs risques.

Cryptoloker, malware, hameçonnage, rançongiciel sont quelques termes qui s'imposent dans les organisations publiques. Ces dernières, victimes d'attaques informatiques, sont parfois dans l'obligation de suspendre leurs services aux citoyens, notamment dans les hôpitaux (Venne, 2019b). L'exemple récent au Québec à Bonjour-santé[2], où une attaque informatique a paralysé le système de prise de rendez-vous pour des malades, démontre les défis de ces transformations. Il faudrait doter les organisations publiques, qui gèrent des données personnelles de millions de citoyens, des moyens de contrôles adéquats pour assurer la maitrise de ces risques. D'où l'importance des audits de cyber-sécurité.

Les audits de cyber-sécurité : une nécessité pour la protection des données

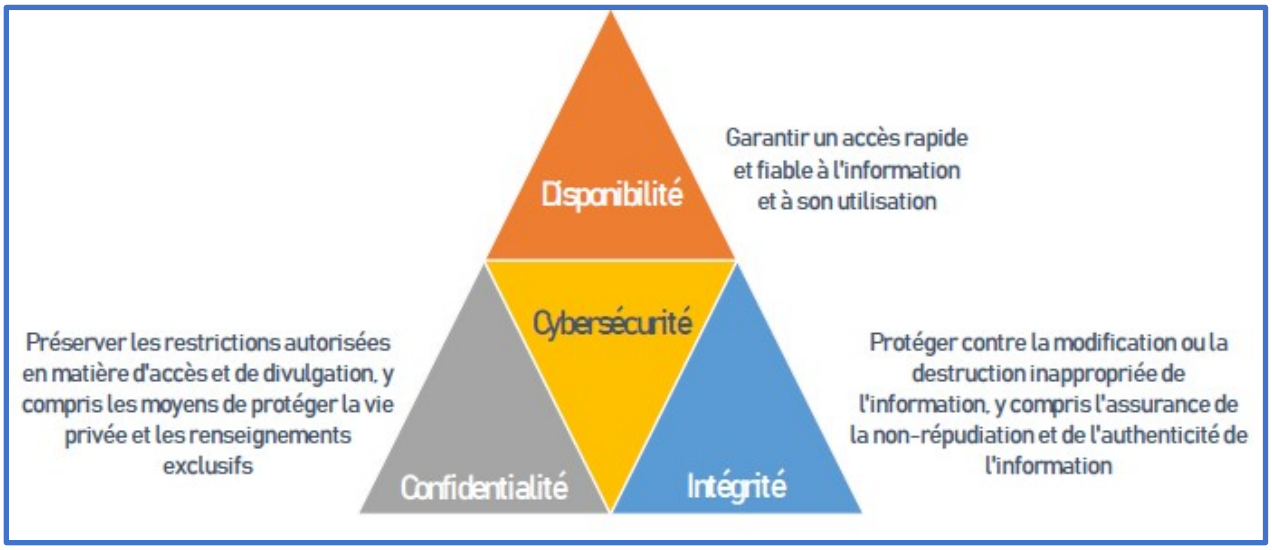
L'évolution de l'audit interne des années 2000 (Charko, 2013) démontre l'intérêt du gouvernement d'optimiser son apport dans la gestion du secteur public. Cependant, selon Piper (2015), la majorité des audits réalisés en Amérique du Nord se consacre aux audits opérationnels (86%), par rapport aux audits des systèmes d'information (54%). En effet, seulement **10%** d'auditeurs internes voyaient en le *e*-commerce un bouleversement dans

[2] Paradis Geneviève, Bonjour-santé toujours paralysé 10 jours après l'attaque informatique, publié le 16 octobre 2019. https://www.tvanouvelles.ca/2019/10/16/bonjour-sante-toujours-paralyse-10-jours-apres-lattaque-informatique, Consulté le 18 octobre 2019.

leurs façons de faire et la plupart pensait que la délivrance électronique des services à la population n'introduirait pas de nouveaux risques (Nikoloyuk *et coll*. 2005). Les piratages actuels devraient avoir changé cette vision.

La cyber-sécurité est « la protection des actifs informationnels en s'attaquant aux menaces pesant sur les informations traitées, stockées et transportées par des systèmes d'information en réseau » (Glossaire-ISACA, 2019). Elle s'occupe de la protection du matériel réseau, des logiciels, la préservation de l'intégrité, la confidentialité et la disponibilité des informations transitant dans l'espace Internet (Henrard, 2019). La cyber-sécurité est une composante de la sécurité des TI.

Figure1 : Objectifs de la cyber-sécurité



Source : Henrard, D. 2019. *L'audit de la cyber-sécurité*. IIA-Canada, p.28

Les attaques informatiques proviennent généralement des accès non-autorisés dans les systèmes informatiques, des modifications malsaines, de l'utilisation abusive ou la destruction d'informations. L'audit de cyber-sécurité est une barrière à ces intrusions, en évaluant les vulnérabilités du système (contrôle des accès, fiabilité des enregistrements, protection des serveurs); en traitant les faiblesses constatées, en vérifiant la conformité aux lois[3], et en donnant aux organes de gouvernance l'assurance que les systèmes concourent à la réalisation des objectifs du ministère/organisme. Basés sur une évaluation des risques

[3] Par exemple veiller à l'application de la Loi sur le Centre de Sécurité des Télécommunications voté en aout 2019.

pertinente, ces audits protègent la confidentialité, l'intégrité, l'accès aux informations des populations et des organisations publiques, protègent les infrastructures contre les cyberattaques et veillent à la continuité des services aux citoyens (FCAR, 2018).

Du fait de la masse et la vitesse de manipulation des données, l'IIA[4] préconise un audit continu de cyber-sécurité, afin « de signaler en temps opportun les lacunes et les faiblesses, pour permettre un suivi et une correction immédiats » (Coderre, 2005 p.2 trad. libre). Pour cela, les auditeurs internes devraient avoir l'expertise dans le domaine. Selon Nikoloyuk *et coll*. (2005), 85% des organisations publiques font appel à l'expertise extérieure dont 45% en audit des TI[5]. Considérant le coût financier de ces expertises, il serait judicieux d'internaliser ce savoir-faire au sein de l'administration publique.

Pour réaliser efficacement des audits de cyber-sécurité, les bonnes pratiques doivent être appliquées : exemple des normes ISO-27000 ou du référentiel COBIT-5[6]. Ce sont des normes spécialisées aux TI, au-delà des normes générales d'audit interne. Leur utilisation exige des techniques que plusieurs auditeurs internes semblent ne pas avoir. Des formations spécialisées sont offertes[7]. L'ISACA[8], organisation par excellence de la gouvernance des TI, offre également des formations et certifications. Elles ne sont pas gratuites, pouvant excéder 3000$ pour les non-membres[9]. Notant les limitations des budgets de formations dans les organisations publiques (Piper, 2015), ces formations ne sont pas disponibles pour tous les professionnels. Le gouvernement pourrait investir davantage. Cet investissement aura un triple bénéfice : armer les auditeurs internes et les membres de comité des compétences pour répondre aux besoins actuels; réaliser un gain d'efficience; assurer un contrôle continu et efficace de l'information. L'étude réalisée par Islam *et coll*. (2018) montre que l'étendue et la qualité des audits de cyber-sécurité dépendent de la compétence des auditeurs, mais aussi du soutien des conseils d'administration.

[4] Institute of Internal Auditors

[5] Bien que cette étude date de près d'une quinzaine d'années, les attaques informatiques récurrentes laissent penser que la situation n'a pas forcément évolué positivement. Pour le Québec notamment, un portrait réalisé par le Secrétariat du Conseil du trésor montre que seulement 14% des ministères et organismes ont réalisé au moins un audit des technologies de l'information en 2017-2018.

[6] Référentiel sur la gouvernance des systèmes d'information

[7] Université de Sherbrooke, programme et admission : DAT811-Audit et contrôle informatique https://www.usherbrooke.ca/admission/fiches-cours/dat811/audit-et-controle-informatique/ consulté le 25 octobre 2019
ESG-UQUAM, Initiation à l'audit informatique https://perfectionnement.esg.uqam.ca/formation/initiation-laudit-informatique/ consulté le 25 octobre 2019

[8] Information System Audit and Control Association

[9] ISACA-Section de Québec, les formations ISACA Québec, COBIT 5 – Certification fondation. https://isaca-quebec.ca/activites/formations/ consulté le 23 octobre 2019

Concernant les membres de comité d'audit, en plus d'exiger qu'au moins un membre ait une expertise financière (Directive sur l'audit interne, art.B.1.2.3), le Contrôleur Général pourrait exiger un membre ayant une certification en audit des TI (CISA[10] ou CRISC[11]).

Conclusion

La transformation numérique apporte des changements dans la vie des citoyens et dans l'administration. Ces changements exposent les organisations publiques à de nouveaux risques, car elles gèrent des informations sensibles. Pour réduire ces risques, les audits de cyber-sécurité devraient être continuellement réalisés. Le gouvernement pourrait davantage investir dans la formation des auditeurs internes et des comités d'audit, pour qu'ils aient l'expertise dans le domaine. Ceci permettra de réduire les coûts liés aux pertes de données, et rassurer les citoyens sur la protection de leurs informations confidentielles. Les technologies de l'information évoluent. L'intelligence artificielle est un autre domaine auquel l'audit interne doit s'adapter.

Bibliographie

Charko, P. 2013. « Management improvement in the Canadian public service: 1999–2010 ». *Canadian Public Administration.* Vol.56, no. 1, pp. 91-120

[10] Certified information system auditor

[11] Certified in risk and information system control

Coderre, D. 2005. « Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment ». *Institute of Internal Auditors / Global technology audit guide (IIA-GTAG).*

Fondation canadienne pour l'audit et la responsabilité (FCAR). 2018. *Pleins feux sur la sécurité des technologies de l'information*. Vigie audit.

Henrard, D. 2019. *L'audit de la cybersécurité*. IIA-Canada, section Québec, 10 et 11 avril.

Institute of Internal Auditors. 2017. *Normes internationales pour la pratique professionnelle de l'audit interne*. https://na.theiia.org/translations/publicdocuments/ippf-standards2017-french.pdf

ISACA. Glossaire. https://www.isaca.org/Pages/Glossary.aspx?tid=2077&char=C

ISACA-section de Québec. https://isaca-quebec.ca/

Islam, M.S.; Nusrat, F.; Stafford, T.F. 2018. « Factors associated with security/cybersecurity audit by internal audit function ». *Managerial Auditing Journal. Vol. 33, no.* 4, pp. 377-409. DOI: http://dx.doi.org.acces.bibl.ulaval.ca/10.1108/MAJ-07-2017-1595

Loiseau, H.; Millette, CA.; Lemay, L. 2013. « La stratégie du Canada en matière de cybersécurité : de la parole aux actes? » *Canadian Foreign Policy Journal.* Vol. 19, no. 2, pp. 144-157, DOI: 10.1080/11926422.2013.805151

Nikoloyuk, G.; Marche, S.; McNiven, J. 2005. « E-commerce impact on Canadian public sector audit practice ». *The International Journal of Public Sector Management*. Vol.18, no. 1, pp. 83-95

Piper, A. 2015. *L'audit dans le secteur public*, CBOK, The IIA Research Foundation.

Secrétariat du Conseil du Trésor du Canada. 2017. *Directive sur l'audit interne*. http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32533

Tremblay, MS. 2011. « Les contrôles », dans N. Michaud (dir.), *Secrets d'États? Les principes qui guident l'administration publique et ses enjeux contemporains.* (pp. 464-485). Québec: Presses de l'Université Laval.

Venne, J-F. 2019a. « À la défense des données des contribuables ». *Gestion*, vol. 44, no.3, pp. 66-69. DOI:10.3917/riges.443.0066.

Venne, J-F. 2019b. « Les établissements des réseaux de la santé dans la mire des pirates ». *Gestion*. Vol. 44, no. 3, pp. 70-73, Doi:10.3917/riges.443.0070.

Welby, B. 2019. « The impact of digital government on citizen well-being ». *OECD Working Papers on Public Governance* No. 32.