Audit de la sécurité des technologies de l'information

Avis aux lecteurs : *Ce rapport contient des renseignements confidentiels, ou bien de l'information liée à la sécurité. En vertu de la Loi sur l'accès à l'information, ces informations ont été caviardées.*

Division de l'audit interne
Conseil de recherches en sciences naturelles et en génie du Canada et Conseil de recherches en sciences humaines du Canada

Approuvé par les présidents le 23 juillet 2021

Also available in English under the title: Audit of Information Technology (IT) Security

Pour obtenir plus de renseignements, veuillez communiquer avec :

Conseil de recherches en sciences naturelles et en génie du Canada
350, rue Albert
Ottawa (Ontario) K1A 1H5
www.nserc-crsng.gc.ca

No de cat. NS3-58/2021F-PDF
ISBN : 978-0-660-40627-5

TABLE DES MATIÈRES

CONTEXTE

Le Conseil des recherches en sciences naturelles et en génie du Canada (CRSNG) et le Conseil de recherches en sciences humaines du Canada (CRSH) (les « Organismes ») sont des organismes ministériels du gouvernement du Canada créés en 1977 et 1978, respectivement. Les Organismes sont financés directement par le Parlement afin d'appuyer la réalisation des projets érudits dans les établissements d'enseignement postsecondaire du Canada et relèvent du Parlement par l'entremise du ministre de l'Innovation, des Sciences et de l'Industrie. Les Organismes relèvent de la Direction des services administratifs communs (DSAC), qui est responsable des services partagés des Ressources humaines, de Finances et administration des octrois et des Solutions d'information et d'innovation (SII).

POURQUOI EST-CE IMPORTANT ?

Le rythme effréné des activités numériques et la transition en cours vers l'infonuagique créent de nouveaux défis pour les entités du secteur privé et public. Les approches à la sécurité traditionnelles des TI doivent évoluer avec les nouveaux contextes, et en agissant sur ces développements, les organismes du gouvernement peuvent améliorer la résilience, mieux appuyer les objectifs opérationnels et réduire le risque d'atteinte à la sécurité des TI.

OBJECTIF ET PORTÉE

L'objectif de cet audit était d'évaluer l'efficacité des aspects précis du cadre de gestion de la sécurité des TI des Organismes, notamment l'efficacité des mesures de protection techniques et opérationnelles dans les domaines de la Politique sur la sécurité des TI, la sensibilisation au sujet de la sécurité des TI, la gestion des risques de sécurité des TI, la gestion de la vulnérabilité du réseau et le développement du système, y compris l'utilisation des données.

La portée de l'audit se concentrait principalement sur les domaines de risque élevé énumérés dans l'Examen préliminaire de la sécurité des TI de 2019 :

- Politique sur la sécurité des TI
- Formation et sensibilisation des utilisateurs sur la sécurité des TI
- Gestion des risques liés à la sécurité des TI
- Gestion des menaces et des vulnérabilités
- Élaboration du système et utilisation des données

Les contrôles qui se situent chez n'importe lequel des fournisseurs des TI à l'extérieur de la DSAC étaient exclus de la portée.

MÉTHODOLOGIE DE L'AUDIT

Lors de la phase de planification, l'équipe de l'audit a effectué une évaluation des risques et une validation de l'information résultant de l'Examen préliminaire de la sécurité des TI de 2019. En se fondant sur cette évaluation, l'équipe a concentré son analyse sur les éléments suivants : politiques de sécurité des TI, rôles et responsabilités, sensibilisation et formation des utilisateurs, gestion des risques, gestion des menaces et vulnérabilités associées aux TI, et données utilisées dans l'élaboration du système.

L'audit a été effectué conjointement par l'équipe de la Division de l'audit interne (DAI) et un fournisseur externe de services d'assurance. La méthodologie pour l'audit comprenait un examen des documents, des entrevues avec la direction et le personnel et des tests des contrôles clés.

La Politique sur l'audit interne du Conseil du Trésor établit les responsabilités des administrateurs généraux du CRSNG/CRSH. Conformément à *Politique sur l'audit interne* du Conseil du Trésor, l'audit a été effectué conformément au Cadre de référence des pratiques professionnelles de l'Institut des vérificateurs internes.

CONSTATATIONS

Lors de l'audit, un nombre de forces associées au programme de sécurité des TI des Organismes a été identifié par l'équipe d'audit, comme suit :

- Les Organismes ont élaboré un plan de sécurité ministériel exhaustif grâce à une approche axée sur les risques, qui comprenait un plan d'action pour améliorer la sécurité des TI des Organismes.
- De nombreux mécanismes et outils sont en place pour identifier les incidents de sécurité des TI au niveau de l'infrastructure, et un processus de gestion des vulnérabilités a été élaboré.
- Les Organismes ont conçu et mis en œuvre une formation en matière de sécurité des TI pour tous les nouveaux employés.
- Les Organismes ont officiellement évalué leur environnement des TI par rapport aux 10 meilleures mesures de sécurité des TI du Centre canadien pour la cybersécurité[1]. Cela comprenait des réponses officiellement documentées pour chaque mesure de sécurité recommandée, avec des plans d'action pour combler tous les écarts.

Lors de l'audit, il a été noté que certains secteurs pouvaient bénéficier d'améliorations à la sécurité des TI, comme suit :

- [caviardé pour des raisons de sécurité]
- [caviardé pour des raisons de sécurité]
- Le processus pour s'assurer que les changements aux systèmes des TI sont correctement suivis, et ensuite évalués du point de vue de la sécurité des TI n'a pas été officialisé ou mis en œuvre. Sans un processus d'évaluation de la sécurité officiellement documenté, il y a plus de risque que des systèmes élaborés et utilisés ne répondent pas aux exigences de sécurité.
- [caviardé pour des raisons de sécurité]
- Un processus pour suivre et gérer les menaces et les vulnérabilités associées aux TI n'est pas en place, et les essais de pénétration ne sont pas effectués au niveau de l'application pour identifier et gérer de façon proactive les vulnérabilités de sécurité des TI. Sans la gestion active des menaces et des vulnérabilités associées aux TI, il y a

[1] https://cyber.gc.ca/fr/10-meilleures-mesures-de-securite-des-ti-0

un plus grand risque que des vulnérabilités importantes ne soient pas réglées en fonction des priorités ou rapidement.

CONCLUSION

La direction a établi un certain niveau des contrôles de la sécurité des TI dans chacun des secteurs de la sécurité des TI qui ont été évalués lors de l'audit ; toutefois, alors que les Organismes continuent de devenir plus numériques, y compris la migration à des technologies plus modernes dans le nuage et autrement, il y a place à amélioration de la façon dont les activités de gestion des risques des TI sont effectuées. [caviardé pour des raisons de sécurité]

RÉPONSE ET PLAN D'ACTION DE LA DIRECTION

ARTICLE	RECOMMANDATION	RÉPONSE ET PLAN D'ACTION DE LA DIRECTION	DATE CIBLE
1.	[caviardé pour des raisons de sécurité]	[caviardé pour des raisons de sécurité]	[caviardé pour des raisons de sécurité]
2.	[caviardé pour des raisons de sécurité]	[caviardé pour des raisons de sécurité]	[caviardé pour des raisons de sécurité]
3.	Il est recommandé que le DPI officialise les processus d'évaluation et d'autorisation de sécurité (EAS) et l'approche, et s'assurer qu'ils sont intégrés de façon appropriée dans le cycle de vie de développement et de maintenance du système des TI. Cela devrait inclure un mécanisme officiel de suivi et de surveillance des activités d'évaluation et d'autorisation de sécurité afin de pouvoir rédiger un rapport et s'assurer que les mesures de protection recommandées sont mises en œuvre rapidement.	Le coordonnateur de la sécurité des TI officialisera, documentera et communiquera le cadre pour le processus d'évaluation et d'autorisation de la sécurité qui comprendra la maintenance et le cycle de vie. Le dirigeant principal de l'information, en collaboration avec le dirigeant principal de la sécurité, s'assurera que le cadre est appliqué au cycle de vie de tous les systèmes.	Mars 2022
4.	[caviardé pour des raisons de sécurité]	[caviardé pour des raisons de sécurité]	[caviardé pour des raisons de sécurité]
5.	Il est recommandé que le DPI élabore davantage son programme pour inclure l'ouverture de session, le classement par ordre de priorité et le suivi des menaces et des vulnérabilités associées aux TI. De plus, une approche axée sur le risque devrait être appliquée lorsqu'on effectue les essais de pénétration dans le portefeuille d'application.	Le coordonnateur de la sécurité des TI s'assurera que le processus actuel est officialisé et documenté afin de consigner et de suivre les menaces et les vulnérabilités associées aux TI. Ce processus capturera la stratégie axée sur les risques lors de la tenue d'essais de pénétration dans l'ensemble du	Mars 2022