29_P-113.2

RESPECT DES OBLIGATIONS EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION DÉCOULANT DE LA LOI SUR LA GOUVERNANCE ET LA GESTION DES RESSOURCES INFORMATIONNELLES DES ORGANISMES PUBLICS ET DES ENTREPRISES DU GOUVERNEMENT

Rapport d'audit

Direction de la vérification interne et de l'évaluation des programmes

Rapport au 8 juin 2023
Présentation au comité actif-passif et audit le 21 juin 2023

Québec

RAPPORT D'AUDIT INTERNE

De la Direction de la vérification interne et de l'évaluation des programmes

Madame la Présidente du comité actif-passif et audit,

Membres du comité actif-passif et audit,

Nous avons procédé à l'audit du respect, par la Société de l'assurance automobile du Québec, des obligations en matière de sécurité de l'information découlant de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, Chapitre G-1.03)*. Cet audit a été réalisé conformément aux dispositions du cadre légal et réglementaire applicables au présent mandat et aux documents de référence fournis par le ministère de la Cybersécurité et du Numérique.

Responsabilités des unités administratives auditées

Les responsabilités en matière de sécurité de l'information sont attribuées à tous les niveaux de l'organisation, incluant notamment les détenteurs et l'ensemble des utilisateurs qui accèdent, utilisent ou gèrent les actifs informationnels de la Société. La sécurité de l'information s'inscrit donc dans un contexte de gestion globale et intégrée, dont la responsabilité est attribuée au chef de la sécurité de l'information organisationnelle.

Responsabilités de l'auditeur interne

Notre responsabilité consiste à fournir une conclusion sur les objectifs propres à la présente mission d'audit en nous basant sur le travail que nous avons réalisé.

Notre audit a été effectué conformément aux *Normes internationales pour la pratique professionnelle de l'audit interne*, élaborées par l'Institut des auditeurs internes. Nos procédés d'audit visaient à recueillir des éléments probants suffisants et appropriés et à les analyser pour fonder nos conclusions et obtenir un niveau d'assurance raisonnable. Les éléments probants ont été obtenus notamment par l'entremise des unités administratives auditées, des entrevues et des observations directes.

Conclusion de l'auditeur interne

Bien que plusieurs forces aient été relevées en matière de sécurité de l'information, notamment au niveau de l'environnement « Patrimoine », nous concluons que les éléments de non-conformité soulevés pourraient compromettre significativement la sécurité de l'information de la Société.

Nos travaux d'audit ont permis de constater que la Société ne répond pas à plusieurs des obligations minimales en matière de sécurité de l'information. En effet, nous avons notamment constaté, au niveau de l'environnement CASA :

- l'absence d'antivirus sur plus de la moitié des serveurs;
- l'absence d'essai de reprise complet à partir des copies de sauvegarde isolées;
- l'utilisation de divers systèmes d'exploitation désuets depuis plusieurs années qui ne sont plus supportés par des mises à jour de sécurité étendue.

Depuis février 2023, la majorité des activités de la Société sont tributaires du fonctionnement de l'environnement CASA. Advenant un incident, la combinaison de ces lacunes pourrait mener jusqu'à un arrêt complet des activités de la Société et des services offerts à la population, et ce, pour une période indéterminée. En effet, les mesures de protection de certains serveurs de l'environnement CASA sont déficientes et il pourrait être difficile, voire même impossible, d'utiliser les copies de sauvegardes prévues à cet effet, car elles ne font l'objet d'aucun essai de reprise complet.

Le directeur de la vérification interne et de l'évaluation des programmes,

[redacted]

Daniel Pelletier, CPA

Québec, 8 juin 2023

MISE EN CONTEXTE

Les révisions de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, chapitre G-1.03)* (ci-après la LGGRI), en juin 2021, et de la Directive gouvernementale sur la sécurité de l'information (ci-après la Directive), en décembre 2021, ont introduit un nouveau modèle de gouvernance de la sécurité de l'information qui vise à :

- renforcer la prise en charge des exigences de sécurité de l'information par les organismes publics;
- contrôler et vérifier les mesures afférentes;
- assurer une réaction rapide et proactive en cas de menaces ou de cyberattaques.

La LGGRI prévoit notamment qu'un organisme public doit, au plus tard le 10 juin 2023 et, par la suite, tous les cinq ans, procéder à un audit portant sur le respect des obligations en matière de sécurité de l'information qui en découlent[1].

RÔLES ET RESPONSABILITÉS

Les responsabilités en matière de sécurité de l'information sont attribuées à tous les niveaux de l'organisation, incluant notamment les détenteurs et l'ensemble des utilisateurs qui accèdent, utilisent ou gèrent les actifs informationnels de la Société. La sécurité de l'information s'inscrit donc dans un contexte de gestion globale et intégrée, dont la responsabilité est attribuée au chef de la sécurité de l'information organisationnelle[2] (ci-après le CSIO).

ÉTENDUE ET PORTÉE DES TRAVAUX

La Direction de la vérification interne et de l'évaluation des programmes (ci-après la DVIEP) a procédé à l'audit du respect, au 30 novembre 2022, de certaines obligations en matière de sécurité de l'information découlant de la LGGRI. Cet audit a été réalisé conformément aux dispositions du cadre légal et réglementaire applicables au présent mandat et aux documents de référence fournis par le ministère de la Cybersécurité et du Numérique (ci-après le MCN).

- Les obligations incluses dans la portée de l'audit sont présentées à l'Annexe 1 du présent rapport. Elles portent sur l'ensemble du processus de gestion de la sécurité de l'information de la Société, de la gouvernance qui encadre ce processus jusqu'à sa mise en application.

Les travaux d'audit ne peuvent suffire à s'assurer de l'efficacité de l'encadrement en matière de sécurité de l'information ni de la prise en charge adéquate et en temps opportun de l'exhaustivité des lacunes en sécurité de l'information. Toutefois, si nos travaux identifiaient des irrégularités ou des lacunes importantes qui n'ont pas été prises en charge, elles seraient incluses dans notre audit.

[1] LGGRI, article 16.6.2

[2] Attribution en vertu de l'article 10 de la Directive

Le mandat d'audit permet de conclure sur la conformité à certaines obligations en matière de sécurité de l'information découlant de la LGGRI en date du 30 novembre 2022, mais il peut également faire référence à des situations antérieures ou ultérieures à cette date, le cas échéant.

> L'expression *« en conformité avec les obligations en matière de sécurité de l'information découlant de la LGGRI »* signifie que les pratiques en sécurité de l'information de la Société, prises dans leur ensemble, satisfont aux obligations de la LGGRI posées par les différentes références légales et réglementaires et bonnes pratiques associées aux obligations incluses dans la portée de l'audit.

Les procédés d'audit visaient à recueillir les éléments probants suffisants et appropriés et à les analyser pour fonder les conclusions sur les objectifs d'audit et pour obtenir un niveau d'assurance raisonnable. Les éléments probants ont été obtenus notamment par l'entremise des unités administratives auditées, des entrevues et des observations directes.

Les travaux d'audit ont été menés conformément aux *Normes internationales pour la pratique professionnelle de l'audit interne*, élaborées par l'Institut des auditeurs internes.

En conformité avec ces normes, la position et le rattachement fonctionnel de la DVIEP dans la Société lui ont permis d'exercer ses fonctions de façon indépendante. Ainsi, ses travaux ont été conduits de façon professionnelle et objective.

DIFFICULTÉS RENCONTRÉES LORS DES TRAVAUX D'AUDIT

Délais octroyés

Bien que le présent audit ait pour objectif d'évaluer la conformité aux obligations découlant de la LGGRI en date du 30 novembre 2022, les précisions du MCN concernant sa portée n'ont été transmises à la haute direction de la Société que le 15 décembre 2022 et la DVIEP n'en a été avisée qu'en février 2023. Ainsi, les travaux d'audit de la DVIEP ont été restreints dans le temps et certaines informations historiques n'ont pu être obtenues afin de conclure sur la conformité au 30 novembre 2022.

La planification d'un tel mandat aurait dû être entamée au début de l'automne 2022 afin de permettre à la DVIEP une meilleure prise de connaissance des éléments à vérifier, mais également d'augmenter leur étendue.

Portée et étendue de l'audit

Les précisions du MCN concernant la portée de l'audit permettaient de circonscrire les éléments à auditer à certaines obligations découlant de la LGGRI, mais pas de préciser l'étendue des travaux d'audit à effectuer. Ainsi, pour certains éléments, la DVIEP a dû évaluer s'il lui était possible, dans les délais impartis, d'effectuer un audit plus approfondi ou si elle devait concentrer ses travaux sur les critères minimums prédéfinis par le MCN.

Confidentialité des informations

Pour des raisons de confidentialité évoquées par la Direction générale de la sécurité de l'information (ci-après la DGSI), plusieurs documents supportant les activités en matière de sécurité de l'information n'ont pas été transmis à la DVIEP. Certains lui ont été présentés lors de rencontres virtuelles aux fins d'observation seulement. Par conséquent, les auditeurs tiennent à informer les lecteurs que certains travaux d'audit se sont arrêtés à la validation de l'existence des

éléments à vérifier, ce qui exclut donc la validation de l'exactitude et de l'exhaustivité des informations présentées et de l'efficacité des outils utilisés pour mener à bien les activités de la Société en matière de sécurité de l'information. En effet, il est difficile pour un auditeur d'émettre une opinion basée seulement sur des observations[3].

Considérant ces difficultés, la DVIEP a précisé l'étendue de son audit de certains éléments soit directement dans le constat concerné ou en notes de bas de page dans l'Annexe 1.

OBJECTIF DE L'AUDIT

Le présent audit vise à s'assurer du respect de certaines obligations en matière de sécurité de l'information découlant de la LGGRI en date du 30 novembre 2022. Les obligations à considérer aux fins de l'audit ont été préétablies par le MCN. Elles sont regroupées en 13 sections et leur détail a été reporté à l'Annexe 1 :

1. Gouvernance;
2. Encadrement;
3. Événements de sécurité;
4. Inventaire des actifs informationnels;
5. Désuétude;
6. Vulnérabilités;
7. Reprise informatique;
8. Confidentialité;
9. Surveillance;
10. Formation;
11. Gestion des identités et des accès;
12. Accès aux services gouvernementaux;
13. Antivirus.

Chacune de ces obligations a fait l'objet d'une évaluation basée sur les critères minimums prédéfinis par le MCN découlant des références légales et réglementaires et des bonnes pratiques en matière de sécurité de l'information suivantes :

- *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement;*
- *Directive gouvernementale sur la sécurité de l'information;*
- *Bilan en sécurité de l'information;*
- *Les 15 mesures minimales de sécurité* identifiées par le Centre gouvernemental de cybersécurité;
- *Processus gouvernemental de gestion des menaces, des vulnérabilités et des incidents.*

Les constats et recommandations présentés dans ce rapport visent à répondre aux objectifs de l'audit.

- Afin d'améliorer la qualité de la sécurité de l'information de la Société, quelques opportunités d'amélioration ont été identifiées.
- Afin d'en assurer la continuité, les forces et bonnes pratiques réalisées par la Société ont aussi été identifiées.

[3] Selon la *Directive sur l'audit interne dans les ministères et les organismes* adoptée en janvier 2021, la fonction d'audit interne doit avoir un accès direct et non restreint à tous les employés de l'organisation, lieux, bases de données, systèmes informatiques, informations, explications et à toute autre documentation nécessaire à la réalisation de ses travaux.

FORCES RELEVÉES

Les travaux réalisés ont mené à l'identification de plusieurs forces qui permettent à la Société de se conformer à certaines obligations de la LGGRI, notamment au niveau de l'environnement « Patrimoine ». Ces forces émanent principalement des pièces justificatives fournies à la DVIEP pour les fins de l'audit et des renseignements transmis lors des entrevues menées[4].

FORCE 1 - Depuis plusieurs années, la Société bénéficie d'une direction générale dédiée à la sécurité de l'information. Les activités de cette direction générale sont encadrées par le *Cadre de gestion de la sécurité de l'information* (ci-après le Cadre SI), adopté en 2016, et la *Politique sur la sécurité de l'information* (ci-après la Politique SI), mise à jour en 2019. Ces documents définissent notamment les responsabilités essentielles en matière de sécurité de l'information.

FORCE 2 - Le comité sur la sécurité de l'information est la principale instance de concertation en matière de sécurité de l'information à la Société depuis plusieurs années. Il implique, notamment, les responsables sectoriels de la sécurité de l'information et des représentants des unités responsables des technologies de l'information, de la vérification interne, de l'accès à l'information et de la protection des renseignements personnels, de la gestion documentaire, de la sécurité physique et de l'éthique.

FORCE 3 - Il y a plusieurs années, la Société a mis en place un comité de gestion de crise qui relève directement du président-directeur général. En cas de sinistre avéré, la structure de gestion de crise de la Société remplace le comité de direction pour se charger, entre autres, de procéder à l'évaluation des dommages, d'assurer la mise en œuvre du plan de continuité et d'assurer la coordination avec les intervenants de l'extérieur de la Société. Les intervenants clés en sécurité de l'information sont prévus dans le plan de gestion de crise.

FORCE 4 - En 2019, la Société a créé un Centre opérationnel de cyberdéfense (ci-après le COCD). Le COCD a pour mission de prévenir les cyberattaques, sinon de les traiter afin de réduire leurs impacts sur le bon déroulement des activités de la Société et ainsi assurer la continuité des services offerts aux citoyens.

FORCE 5 - La Société met à la disposition des employés de la Société plusieurs directives internes indiquant la marche à suivre lors de la réception de courriels malicieux, la détection de virus ou en présence d'autres menaces.

Une page de l'intranet de la Société est dédiée à la sécurité de l'information. Cette page présente, entre autres, la marche à suivre en cas de :

- Réception d'un courriel suspect;
- Réception de communication frauduleuse;
- Comportement inhabituel du poste de travail;
- Perte d'un support informatique ou bris de confidentialité.

[4] Les travaux d'audit se sont arrêtés à la validation de l'existence des informations présentées, car il n'a pas toujours été possible pour la DVIEP de valider l'exhaustivité et l'exactitude de ces informations.

FORCE 6 - La documentation du processus de la gestion des événements d'intérêts[5] est effectuée de manière claire et précise par le COCD.

Une documentation claire et complète est la pierre angulaire d'une organisation de travail précise et de qualité. Elle démontre la transparence d'une organisation, facilite les suivis et permet de conserver la mémoire organisationnelle.

La DVIEP a pu observer que :

— le processus de gestion des événements de sécurité est clairement défini dans le *Plan de réponse aux incidents de sécurité de l'information numérique*;

— la documentation du suivi des événements d'intérêt est effectuée de manière claire et précise.

FORCE 7 - La Société s'est dotée du système [redacted] qui, au terme de son implantation, lui permettra d'obtenir en temps réel l'inventaire de ses actifs informatiques et de tout actif qui se connecte sur ses systèmes.

En date du 30 novembre 2022, la majorité des actifs informatiques de la Société avaient été intégrés à cet outil. La DGSI finalisera l'intégration de tous les actifs de la Société d'ici la fin de l'année 2023.

FORCE 8 - Le processus de journalisation des événements de la Société est clairement documenté et mis en œuvre.

Le COCD met en œuvre les bonnes pratiques définies dans ses « Règles fonctionnelles de journalisation » élaborées en 2019. Ce document détaille notamment les règles fonctionnelles de journalisation des événements et présente les bonnes pratiques permettant de bâtir une architecture de gestion des journaux, quelle que soit la nature du système d'information.

FORCE 9 - La Société met à la disposition de ses employés trois solutions de courriels sécurisés. Chacune de ces solutions cible des échanges particuliers, dont notamment:

— les échanges d'informations liées à la cybersécurité avec le MCN;

— les échanges d'informations sensibles avec des partenaires ciblés;

— le transfert de fichiers contenant des renseignements confidentiels avec des partenaires externes et/ou des citoyens.

Cette dernière solution est offerte, sur demande, à tous les employés de la Société.

[5] Un événement d'intérêt est tout type d'événement de sécurité qui indique une menace potentielle contre des actifs informationnels d'une organisation. Par définition, de tels événements pourraient indiquer qu'un système d'information, un service ou un réseau est victime d'une brèche informatique et est compromis, qu'une politique de sécurité a été violée, qu'une menace n'a pas été maîtrisée avec succès par les contrôles de sécurité existants, etc.

FORCE 10 - La formation continue est un excellent moyen pour permettre à la Société de sensibiliser les employés sur la sécurité de l'information et ainsi évoluer vers un milieu plus sécuritaire. À cet effet, la Société bénéficie d'un plan de sensibilisation et de formation applicable à tous les intervenants de la Société. Au cours de 2022, la Société a notamment :

- tenu des rencontres d'informations avec les nouveaux gestionnaires et les détenteurs d'actifs informationnels portant sur leurs rôles et responsabilités en sécurité de l'information;
- implanté la plateforme de formation [redacted] qui offre des formations mensuelles obligatoires;
- diffusé plusieurs manchettes de sensibilisation sur l'intranet de la Société portant notamment sur la vigilance face à l'hameçonnage, l'utilisation de clés USB sécurisées, l'augmentation des fraudes en période d'impôts, la protection du mot de passe, les réflexes de sécurité lors du travail en mode hybride;
- transmis des courriels de sensibilisation à l'hameçonnage;
- participé à la campagne gouvernementale de sensibilisation à la cybersécurité.

FORCE 11 - En octobre 2022, la Société a déployé la plateforme [redacted] qui offre des autoformations mensuelles obligatoires. Le contenu offert par cette plateforme permet de renforcer la sensibilisation minimum exigée par le MCN au niveau de la cyberdéfense, mais également d'adapter la sensibilisation en fonction du contexte et des menaces actuels.

FORCE 12 - En juillet 2022, la Société a déposé le dossier d'affaires *Gestion de l'identité et des mécanismes d'authentification – volet 1* (GIMA-1) visant l'amélioration de son processus de gestion des identités et des accès (ci-après la GIA). Ce dossier d'affaires a notamment pour résultats attendus :

- l'élimination de la dette actuelle de la Société en GIA;
- l'alignement avec les orientations technologiques à long terme de la Société;
- le positionnement favorable de la capacité de GIA de la Société vis-à-vis des exigences légales et gouvernementales, des recommandations des auditeurs et des bonnes pratiques de l'industrie.

À terme, ce dossier d'affaires intégrera plusieurs recommandations déjà émises par les auditeurs externes et la DVIEP.

FORCE 13 - Au 30 novembre 2022, la Société offrait à sa clientèle plusieurs mécanismes pour transmettre des informations confidentielles de façon sécuritaire, notamment en remplissant des formulaires en ligne ou en joignant des fichiers.

FORCE 14 - Les antivirus sur les postes de travail et les serveurs supportant l'environnement « Patrimoine » sont à jour et adéquatement contrôlés.

Les entrevues réalisées ont permis de constater que l'ensemble des postes de travail actifs et les serveurs supportant l'environnement « Patrimoine » sont protégés. Des contrôles sont en place pour suivre en temps réel l'état de conformité des antivirus ainsi que pour limiter l'accès aux postes de travail dont l'antivirus est obsolète.

FORCE 15 - Les postes de travail et les serveurs de l'environnement « Patrimoine » sont protégés au-delà du seuil minimal exigé par le MCN. Ils sont protégés par un antivirus qui possède non seulement les fonctionnalités *Endpoint Detection and Response* (ci-après EDR), mais également les fonctionnalités *Data Loss Prevention* (ci-après DLP).

Les fonctionnalités EDR exigées par le MCN permettent la détection d'activités suspectes et virales, tandis que les fonctionnalités DLP permettent de protéger et de sécuriser les données de la Société ainsi que de contrôler leur diffusion.

CONSTATS

Les constats sont présentés en fonction de la priorité des risques selon l'évaluation de la DVIEP. À eux seuls, les quatre premiers constats ont mené la DVIEP à conclure que la sécurité de l'information de la Société pourrait être compromise de façon significative.

CONSTAT 1 - Plus de la moitié des serveurs supportant l'environnement CASA ne sont pas convenablement protégés par un antivirus répondant au seuil minimal exigé par le MCN et à jour

Un antivirus permet de protéger le parc informatique des attaques telles que les virus, les logiciels malveillants et les cybermenaces. Une attaque pourrait notamment générer le ralentissement du parc informatique de la Société, le vol, la corruption ou la perte de ses données ainsi que l'incapacité de fournir ses services aux citoyens.

Bien que les serveurs supportant l'environnement « Patrimoine » soient adéquatement protégés, ce n'est pas le cas pour plus de la moitié de ceux supportant l'environnement CASA.

Les travaux d'audit ont permis de constater qu'au niveau de l'environnement CASA :

- en date du 26 avril 2023[6], aucun antivirus n'avait été déployé sur près de 50 % des serveurs[7];
- les serveurs protégés n'étaient pas munis d'un antivirus comprenant les fonctionnalités EDR. Ainsi, l'antivirus utilisé n'est pas suffisant, car il ne permet pas la détection d'activités suspectes et virales;
- en date du 24 février 2023[8], 13 % des serveurs protégés n'étaient pas protégés par un antivirus à jour ou l'antivirus était de statut inconnu.

Selon les informations obtenues, l'antivirus proposé par l'intégrateur pour protéger l'environnement CASA ne s'est pas avéré fonctionnel sur une partie des serveurs. À la suite à l'intervention de la DGSI, un autre produit a été proposé et testé. La solution retenue est en cours de déploiement.

Recommandation

R.1 Déployer rapidement un antivirus muni des fonctionnalités EDR sur l'ensemble des serveurs supportant l'environnement CASA et s'assurer qu'il est maintenu à jour.

Actions prévues par la vice-présidence l'expérience numérique (ci-après VPEN)	Responsables	Échéance
Définir la solution et procéder à l'acquisition de 1600 licences antivirus pour les serveurs non conformes ([redacted]-EDR)	DGSI	Terminé
Déploiement de la solution [redacted]-EDR dans le cycle actuel	DGIT DGSI	Septembre 2023

6 Il n'a pas a été possible d'obtenir cette information au 30 novembre 2022.

7 590 serveurs virtualisés sous la solution [redacted] et 218 serveurs [redacted] sous [redacted], pour un total de 808 serveurs CASA sur 1 646 serveurs CASA.

8 Il n'a pas a été possible d'obtenir cette information au 30 novembre 2022.

CONSTAT 2 - Au niveau de l'environnement CASA, aucun essai de reprise complet n'a été effectué à partir des copies de sauvegarde isolées

Bien que l'environnement CASA soit dupliqué dans un site à Montréal dans le but d'assurer la disponibilité des services, cette duplication ne protège pas la Société contre tous les types de sinistres. Par exemple, advenant la réussite d'une attaque de type « rançongiciel », la reprise informatique de services importants de la Société, notamment SAAQClic, pourrait être compromise.

Afin de se prémunir contre ce type de sinistre, des essais de reprise doivent aussi être réalisés à partir des copies de sauvegarde. Ces copies doivent être préalablement isolées du réseau.

Les travaux d'audit ont permis de constater que :

- certaines composantes de l'environnement CASA ne disposaient pas de copies de sauvegarde isolées;
- aucun essai de reprise complet n'a été réalisé à partir des copies de sauvegarde isolées pour l'environnement CASA. Selon la DGSI, un dossier d'opportunité[9] est en cours.

Recommandations

R.2 S'assurer que l'ensemble des composantes de CASA fasse l'objet de copies de sauvegarde quotidiennes isolées du réseau

R.3 Mettre à jour le plan de reprise afin d'intégrer les essais de reprise à partir de copies de sauvegarde isolées pour l'environnement CASA

R.4 Effectuer des essais de reprise complets à partir des copies de sauvegarde isolées de l'environnement CASA

Action prévue par la VPEN	Responsable	Échéance
Terminer le projet P13-12108 : Continuité des affaires. Le dossier d'affaires qui fait suite au dossier d'opportunité approuvé sera bonifié au niveau de la reprise informatique afin de couvrir les différents scénarios de sinistres, notamment la reprise des services numériques utilisant les sauvegardes. Le dossier d'affaires sera soumis pour approbation au cours des prochaines semaines. Le projet répond aux recommandations : — S'assurer que l'ensemble des composantes de CASA fasse l'objet de copies de sauvegarde quotidiennes isolées du réseau — Mettre à jour le plan de reprise afin d'intégrer les essais de reprise à partir de copies de sauvegarde isolées pour l'environnement CASA — Effectuer des essais de reprise complets	DGSI	2024

[9] Un dossier d'opportunité présente l'information nécessaire à une prise de décision éclairée face à un projet qualifié en ressources informationnelles. Un dossier d'opportunité est à l'étape d'évaluation et non en réalisation.

CONSTAT 3 - Le plan de mitigation des vulnérabilités prévu par la Société pour les systèmes d'exploitation désuets sur les serveurs ne couvre pas les systèmes d'exploitation [redacted] actuellement désuets à la Société

Afin de s'assurer de diminuer les vulnérabilités sur les systèmes d'exploitation désuets sur ses serveurs, le plan de mitigation de la Société prévoit l'utilisation des mises à jour de sécurité étendue offertes par les manufacturiers.

Une mise à jour de sécurité étendue est une option offerte après la fin de vie normale du système d'exploitation[10]. Cette mise à jour ne permet pas d'améliorer le système d'exploitation, ni d'y ajouter des fonctionnalités, mais seulement d'apporter des correctifs aux vulnérabilités découvertes en attendant le rehaussement du système d'exploitation.

Les travaux d'audit ont permis de constater que les mises à jour de sécurité étendues ne sont pas offertes pour les systèmes d'exploitation [redacted] actuellement désuets sur les serveurs de la Société. Ainsi, en date du 30 novembre 2022, la DVIEP a retracé au moins 20 serveurs disposant de systèmes d'exploitation désuets non supportés par des mises à jour de sécurité étendue depuis au moins 2 ans.

Recommandations

R.5 Procéder rapidement au rehaussement ou au remplacement des systèmes d'exploitation [redacted] désuets

R.6 Mettre à jour le plan de mitigation afin de l'adapter à tous les types de systèmes d'exploitation

Actions prévues par la VPEN	Responsables	Échéance
Élaborer la stratégie de rehaussement des systèmes d'exploitation [redacted] désuets	DGIT DGSI	2024
Effectuer le rehaussement ou le remplacement le cas échéant.		
Inclure tous les systèmes d'exploitation [redacted] dans le plan de mitigation		

[10] Cette fin de vie met normalement fin au support standard offert par le manufacturier.

CONSTAT 4 - Le plan de mitigation des vulnérabilités prévu par la Société pour les systèmes d'exploitation [redacted] n'a pas été réalisé en temps opportun

Les travaux d'audit ont permis de constater qu'au 30 novembre 2022, au moins 4 mises à jour disponibles n'avaient pas été installées afin de corriger les vulnérabilités des systèmes d'exploitation [redacted] et qu'elles ne l'étaient toujours pas au 15 mars 2023.

Selon les informations obtenues lors des travaux d'audit, la Société utilise 177 serveurs [redacted] qui ne bénéficiaient pas des dernières mises à jour. Parmi ces serveurs, plusieurs supportent la prestation électronique de services.

Recommandation

R.7 S'assurer d'un suivi régulier des mises à jour de sécurité liées aux systèmes d'exploitation afin de les installer en temps opportun

Action prévue par la VPEN	Responsable	Échéance
Effectuer une assurance qualité relative à l'application des mises à jour de sécurité liées aux systèmes d'exploitation.	DGIT	2024

[11] Le support du système d'exploitation [redacted] s'est terminé en [redacted]

CONSTAT 5 - Les délais de traitement des vulnérabilités en fonction de leur criticité établis par la Société ne sont pas toujours respectés

Bien que la Société se soit dotée d'une *Norme sur la gestion des vulnérabilités et des tests d'intrusion* établissant les délais de traitement des vulnérabilités en fonction de leur criticité, les travaux d'audit ont permis de constater que les délais établis ne sont pas respectés. En effet :

- la DVIEP a retracé au moins 20 serveurs disposant de systèmes d'exploitation désuets non supportés par des mises à jour de sécurité étendue depuis au moins 2 ans[12];
- au 30 novembre 2022, au moins 4 mises à jour disponibles n'avaient pas été installées afin de corriger les vulnérabilités des systèmes d'exploitation [redacted] et elles ne l'étaient toujours pas au 15 mars 2023[13];
- plus de la moitié des serveurs supportant l'environnement CASA n'est pas convenablement protégé par un antivirus répondant au seuil minimal exigé par le MCN et à jour[14].

Recommandation

R.8 S'assurer de respecter les délais de traitement des vulnérabilités en fonction de leur criticité, conformément à la *Norme sur la gestion des vulnérabilités et des tests d'intrusion* de la Société

Actions prévues par la VPEN	Responsables	Échéance
Obtenir l'approbation de la *Directive sur la gestion des vulnérabilités et des tests d'intrusion* et de la *Norme sur la gestion des vulnérabilités et des tests d'intrusion*	DGSI	2023
Informer la DGIT de l'approbation de la *Directive sur la gestion des vulnérabilités et des tests d'intrusion* et de la *Norme sur la gestion des vulnérabilités et des tests d'intrusion* afin que les corrections de vulnérabilités soient prises en charge	DGIT DGSI	2024

[12] Voir le constat 3 pour plus de détails.

[13] Voir le constat 4 pour plus de détails.

[14] Voir le constat 1 pour plus de détails.

CONSTAT 6 - La révision périodique des accès aux privilèges élevés/administrateur n'est pas complète et sa fréquence est insuffisante

Lors des audits effectués en 2019 et 2020, les auditeurs externes ont constaté certaines lacunes ayant trait au processus de gestion des droits et des profils d'accès à privilèges élevés/administrateur. À la suite des rapports d'audit émis, des plans d'action ont été déposés afin de mettre en place de mesures correctrices. En date du présent rapport, certaines des mesures prévues n'avaient toujours pas été mises en place, dont notamment:

— la révision et la mise en œuvre de la procédure encadrant l'accès aux comptes à hauts privilèges pour le support [redacted];

— la fréquence de la révision des accès à hauts privilèges;

— la révision périodique des accès des comptes d'administration des serveurs [redacted]

Recommandations

R.9 Réviser et mettre en œuvre la procédure encadrant l'accès aux comptes à hauts privilèges pour le support [redacted]

Actions prévues par la VPEN	Responsable	Échéance
Réviser et mettre en œuvre la procédure encadrant l'accès aux comptes à hauts privilèges pour le support [redacted]	DGSI	2023

R.10 Réviser plus d'une fois par année l'ensemble des accès à privilèges élevés/administrateur

Actions prévues par la VPEN	Responsable	Échéance
Le projet GIMA prévoit la création de la *Directive sur la gestion des identités et des accès* qui inclut une révision de l'ensemble des accès à hauts privilèges au minimum 2 fois par année	DGSI	2024
Procéder à une révision, plus d'une fois par année, de l'ensemble des accès à hauts privilèges incluant ceux de [redacted] et [redacted]		

CONSTAT 7 - Les degrés de tolérance de la Société face à une interruption des services des technologies de l'information ne sont pas adéquatement déterminés

Afin d'établir les objectifs d'une reprise informatique réussie, une organisation doit définir ses degrés de tolérance face à une interruption de services des technologies de l'information. Ces degrés de tolérance se traduisent par les paramètres suivants :

- Perte maximale de données[15] ;
- Durée maximale d'interruption[16];
- Objectif du délai de reprise[17].

Les degrés de tolérance à l'interruption des services des technologies de l'information se doivent d'être déterminés avec minutie, mais surtout avec l'accord de l'ensemble des lignes d'affaires de la Société.

Les travaux d'audit ont permis de constater que seul l'objectif de délai de reprise est pris en compte pour déterminer les degrés de tolérance de la Société face à une interruption des services des technologies de l'information. Ainsi, les degrés de tolérance déterminés par la Société ne tiennent pas compte de la perte maximale de données ni de durée maximale d'interruption.

Par ailleurs, un rapport précédent[18] de la DVIEP présente un constat à ce sujet. Ce constat mentionne notamment que le délai maximal d'interruption n'était pas défini dans le plan de continuité des activités de la Société. Un plan d'action a été déposé et des mesures correctrices devront être mises en œuvre. En date du présent rapport, la réalisation de la stratégie et la mise à jour de l'analyse des impacts d'affaires (ci-après le BIA) sont toujours en cours.

Recommandation

R.11 Déterminer, de concert avec les lignes d'affaires, tous les paramètres de tolérance de la Société face à une interruption de services des technologies de l'information.

Action prévue par la VPEN	Responsable	Échéance
Tous les paramètres de tolérance de la Société face à une interruption de services des TI sont traités dans le bilan d'impact sur les affaires, en cours de réalisation dans le cadre du projet P13-12108 : Continuité des affaires.	DGSI	2024

[15] La perte maximale de données représente le point à partir duquel les informations utilisées par une activité doivent être restaurées afin de permettre son fonctionnement à la reprise.

[16] La durée maximale d'interruption acceptable définit le temps nécessaire pour que les impacts défavorables pouvant découler de l'interruption d'un service deviennent inacceptables.

[17] L'objectif du délai de reprise concerne quant à lui la durée après un incident durant laquelle un service doit être repris.

[18] Voir la recommandation 5A du rapport d'audit interne – Sécurité de l'information Phase 1 déposé au CTIC-CAPV en mars 2021.

CONSTAT 8 - Un bilan de sécurité a été transmis sans validation préalable par la DVIEP.

Dans le cadre de la collecte d'informations de janvier 2023, la DGSI a transmis au MCN le Bilan de sécurité de l'information (ci-après le Bilan) de la Société portant sur la prise en charge de certaines exigences de la sécurité de l'information au 30 octobre 2022.

La page d'identification de ce Bilan mentionne que les réponses et les pièces justificatives les supportant doivent faire l'objet d'une validation par l'unité administrative de l'audit interne. Cette validation implique de conclure sur la véracité des informations transmises dans le Bilan.

- La DVIEP n'a pas été consultée pour effectuer un mandat de validation du Bilan transmis en janvier 2023;
- Le Bilan transmis ne fait pas mention de l'absence de validation par la DVIEP.

Il est à noter que selon les procédures transmises par le MCN, la validation par l'auditeur interne n'est pas obligatoire à ce jour, mais fortement recommandée.

Recommandation

R.12 Aviser le MCN que le Bilan transmis en janvier 2023 n'a pas fait l'objet d'une validation de la part de la DVIEP.

Action prévue par la VPEN	Responsable	Échéance
La Société avisera le MCN que le Bilan transmis en janvier 2023 n'a pas fait l'objet d'une validation de la part de la DVIEP	DGSI	2023

CONSTAT 9 - Les employés de la Société ne sont pas tous sensibilisés sur le besoin d'utiliser un moyen de transfert sécuritaire des données confidentielles lors d'échanges externes

Sensibiliser les employés aux risques liés aux échanges de données confidentielles et les informer sur les outils disponibles permet de réduire le risque de fuite de données sensibles.

Bien que des solutions de courriels sécurisés soient en place depuis plusieurs années au sein de la Société, celles-ci ne sont pas toujours utilisées lorsque nécessaires. En effet, la DVIEP a émis un constat à ce sujet dans un rapport précédent[19] indiquant que certaines informations personnelles étaient échangées entre le secteur des ressources humaines de la Société et une autre organisation sans l'utilisation d'une solution sécurisée. À la suite de ce rapport, un plan d'action a été déposé et des mesures correctrices devront être mises en œuvre.

Recommandation

R.13 Élaborer et mettre en œuvre un plan de sensibilisation ayant trait aux risques liés au transfert sécuritaire de données confidentielles et aux solutions sécuritaires disponibles à la Société.

Actions prévues par la VPEN	Responsables	Échéance
Faire des activités de sensibilisation ciblées portant sur l'échange sécuritaire de renseignements confidentiels	DGSI	2023

[19] Voir le constat 4 du rapport d'audit interne en sécurité de l'information – Phase 2 déposé au CAPV en juin 2022.

CONSTAT 10 - La Société n'a pas procédé aux exercices de simulation d'hameçonnage prévus avant le 30 novembre 2022

Une simulation d'hameçonnage est la meilleure façon de sensibiliser les employés sur les risques et d'identifier ceux les plus susceptibles de se faire prendre au piège. Elle permet également d'intégrer la sensibilisation à la cybersécurité de façon interactive et informative.

Selon son *Plan d'action 2022 - Formation et sensibilisation à la sécurité de l'information*, la Société prévoyait la réalisation d'au moins quatre exercices d'hameçonnage au cours de l'année 2022. La réalisation de ces exercices était liée à l'implantation de la plateforme de formation [redacted] qui ne s'est concrétisée qu'à la fin d'octobre 2022. Ainsi, le premier exercice de simulation n'a eu lieu qu'à la mi-décembre 2022.

Le plan d'action 2023 prévoit également la réalisation d'au moins 4 exercices de simulation d'hameçonnage.

Recommandation

R.14 S'assurer de réaliser les exercices de simulation d'hameçonnage prévus au *Plan d'action - Formation et sensibilisation à la sécurité de l'information*.

Action prévue par la VPEN	Responsable	Échéance
Mise en œuvre de 4 exercices d'hameçonnage	DGSI	2023

CONSTAT 11 - Certaines exigences de la Politique SI et du Cadre SI de la Société ne sont pas entièrement mises en œuvre en date du 30 novembre 2022

En mars 2021, la DVIEP a déposé un rapport d'audit interne[20] ayant notamment pour objectif de conclure sur la mise en application et le suivi du Cadre SI et de la Politique SI adoptés par la Société. Ce rapport présentait des constats et recommandations. Les progrès du plan d'action soumis par les unités administratives auditées sont suivis annuellement.

Le suivi des progrès déposé au CAPA en février 2023 démontrait que certaines recommandations étaient en cours de réalisation ou n'étaient pas réalisées à la satisfaction de la DVIEP :

- La catégorisation de l'ensemble des actifs informationnels était en cours de réalisation. La réalisation de cette action est prévue en 2023;
- Le plan de continuité des activités de la Société n'avait pas été mis à jour à la satisfaction de la DVIEP. En effet, l'analyse et la révision de la stratégie du plan de reprise ainsi que la réalisation de la stratégie et de la mise à jour de la cible du BIA n'étaient pas terminées, bien que l'échéance prévue au plan d'action soit atteinte.

Recommandations[21]

R.15 S'assurer que l'ensemble des actifs informationnels de la Société, autant numérique que non numérique, est catégorisé;

R.16 Mettre à jour le plan de continuité des activités afin d'identifier les activités essentielles de la Société ainsi que leur délai maximal d'interruption.

Actions prévues par la VPEN	Responsable	Échéance
Approbation et publication des versions mises à jour de la Politique et du Cadre de gestion de la sécurité de l'information	DGSI	2023

[20] Rapport d'audit interne en sécurité de l'information – Phase I déposé au CTIC-CAPV en mars 2021.

[21] Ces recommandations proviennent du rapport d'audit en sécurité de l'information – Phase I déposé au CTIC-CAPV en mars 2021. Seules les recommandations liées aux actifs TI en production au 30 novembre 2022 ont été reportées dans le présent rapport.

CONSTAT 12 - En date du 30 novembre 2022, plusieurs documents encadrant les activités en sécurité de l'information[22] de la Société n'avaient pas été mis à jour afin de se conformer aux dernières exigences de la LGGRI et de la Directive

La LGGRI et la Directive ont fait l'objet de plusieurs mises à jour depuis l'adoption du Cadre SI de la Société en 2016 et de sa Politique SI en 2019.

Il est primordial que les documents encadrant la sécurité de l'information évoluent en s'arrimant avec les lois, règlements, directives et orientations du gouvernement ainsi qu'avec les meilleures pratiques en la matière.

Les travaux d'audit ont permis de constater qu'en date du 30 novembre 2022, la Politique SI, le Cadre SI et l'organigramme présentant la structure de gouvernance de la sécurité de l'information de la Société n'avaient pas été mis à jour afin de répondre aux exigences de la LGGRI et de la Directive notamment au niveau des principaux intervenants en sécurité de l'information et de leurs rôles et responsabilités[23].

Recommandations

R.17 Mettre à jour la Politique SI et le Cadre SI afin de respecter les exigences de la LGGRI et de la Directive. Cette mise à jour doit notamment comprendre :

a. l'identification et la définition claire des responsabilités des intervenants principaux en sécurité de l'information en conformité avec celles exigées dans la LGGRI et la Directive.

- Ces rôles et responsabilités doivent également être en conformité avec la structure de gouvernance de la sécurité de l'information présentée dans le *Cadre gouvernemental de gestion de la sécurité de l'information*;

b. la structure de gouvernance de la sécurité de l'information de la Société, sous forme d'organigramme, présentant les principaux intervenants en sécurité de l'information. Cet organigramme doit être adapté au fait que la Société dispose de son propre dirigeant de l'information et que celui-ci assume les fonctions de chef délégué de la sécurité de l'information (ci-après le CDSI) et de CSIO.

R.18 S'assurer que la Politique SI et le Cadre SI sont revus et mis à jour de manière régulière et dès l'apparition de nouvelles exigences légales et réglementaires.

Actions prévues par la VPEN	Responsable	Échéance
Approbation et publication des versions mises à jour de la Politique et du Cadre de gestion de la sécurité de l'information	DGSI	2023

[22] Les documents encadrant la sécurité de l'information comprennent notamment le Cadre SI, la Politique SI, son processus et l'organigramme présentant la structure de gouvernance de la sécurité de l'information.

[23] Dans le cadre de ce mandat, la DVIEP n'a pas comparé l'intégralité des exigences de la LGGRI et de la Directive au Cadre SI et à la Politique SI de la Société. Il est de la responsabilité de la DGSI de s'assurer que son Cadre SI et sa Politique SI respectent l'exhaustivité des exigences légales et réglementaires.

CONSTAT 13 - L'attribution de la fonction de CSIO au sein de la Société ne respecte pas les exigences de la Directive

Les dernières mises à jour de la LGGRI et de la Directive ont mené à la modification de la structure de gouvernance de la sécurité de l'information gouvernementale. Cette modification comprend notamment la création et la modification des fonctions clés en matière de sécurité de l'information.

En vertu des exigences de la Directive, la Société devait procéder à la création et à l'attribution de la fonction de CSIO. Cette fonction assume la responsabilité de la prise en charge globale de la sécurité de l'information au sein de la Société.

- La Société disposant de son propre dirigeant de l'information[24], la fonction de CSIO est attribuée *de facto* à son CDSI[25].
- Les exigences de la Directive ne prévoient pas la possibilité de déléguer cette fonction.

La création et l'attribution formelle des fonctions clés au sein d'une organisation sont essentielles notamment afin de :

- définir clairement les rôles et responsabilités liées à une fonction;
- informer les intervenants concernés et s'assurer de leur imputabilité;
- s'assurer de l'atteinte des objectifs de la Société;
- s'assurer du respect des exigences légales et réglementaires.

Les travaux d'audit ont notamment permis de constater que :

- La fonction de CSIO, bien qu'attribuée initialement au CDSI dans le registre d'autorité de la Société, a été déléguée à un membre du personnel d'encadrement de septembre 2022 à mars 2023;
- En janvier 2023, lorsque la Société a transmis son Bilan, le CDSI se devait d'y apposer sa signature afin d'attester qu'il a vérifié la conformité des réponses et des pièces les justifiant.
    - Bien que cette fonction soit imputée au dirigeant de l'information, en respect des exigences de la LGGRI et selon le registre d'autorité de la Société, le Bilan transmis porte la signature d'un membre du personnel d'encadrement autre que le dirigeant de l'information qui se désigne comme étant le CDSI de la Société.

De plus, il n'a pas été possible d'obtenir les documents probants suffisants et appropriés appuyant la création et l'attribution formelles des fonctions de CSIO et de CDSI au sein de la Société.

[24] En application de l'article 8 de la LGGRI.

[25] Le dirigeant de l'information de la Société agit à titre de CDSI en vertu du paragraphe 9.1° du premier alinéa de l'article 10.1 de la LGGRI.

Recommandations

R.19 Élaborer et mettre en place un processus formel de création et d'attribution des fonctions clés en matière de sécurité de l'information, dont notamment les fonctions de CSIO et de CDSI. Le processus formel doit inclure notamment la mise à jour du registre d'autorité;

R.20 Procéder à la création formelle des fonctions de CSIO et de CDSI, les attribuer formellement au dirigeant de l'information et informer ce dernier des responsabilités liées à ces fonctions.

Actions prévues par la VPEN	Responsables	Échéance
À la suite de l'approbation de la Politique et au Cadre de gestion de sécurité de l'information, élaborer un processus formel de création et d'attribution des fonctions clés en matière de sécurité de l'information	DGSI	2024
Procéder à la création formelle des fonctions de CSIO et de CDSI, les attribuer formellement au dirigeant de l'information et informer ce dernier des responsabilités liées à ces fonctions	Président-directeur général	2023

CONSTAT 14 - La Société n'a pas déployé d'authentification multifacteur pour sécuriser l'accès, via Internet, des commerçants et des mandataires en vérification mécanique à certains systèmes de la Société

Le déploiement de l'authentification multifacteur permet à la Société de diminuer les risques d'accès non autorisés à ses actifs informationnels.

Les travaux d'audit ont permis de constater qu'au 30 novembre 2022, les commerçants et des mandataires en vérification mécanique pouvaient accéder aux systèmes de la Société via Internet sans une authentification multifacteur.

Cependant, depuis le 20 février 2023, les commerçants et mandataires en vérification mécanique doivent premièrement s'authentifier via le Service d'authentification gouvernementale (ci-après le SAG) afin d'accéder aux systèmes de la Société. Le SAG possède un mécanisme d'authentification multifacteur. Ainsi, en date du présent rapport, la Société répond à l'exigence et aucune action supplémentaire n'est jugée nécessaire.

CONSTAT 15 - Le processus de gestion des événements de sécurité de la Société n'a pas été mis à jour en temps opportun

Bien que le *Plan de réponse aux incidents de sécurité de l'information numérique* de la Société et les procédures effectuées par le COCD comprennent toutes les étapes importantes d'un processus de gestion des événements de sécurité, le plan n'avait pas fait l'objet d'une mise à jour au 30 novembre 2022 afin de :

- intégrer les nouvelles fonctions exigées par la LGGRI et la Directive telles que le CDSI et le CSIO;
- s'harmoniser avec le *Processus de gestion des menaces, des vulnérabilités et des incidents*[26] du Centre gouvernemental de cyberdéfense.

Cependant, une mise à jour comprenant la nouvelle structure organisationnelle et s'harmonisant avec le processus gouvernemental a été approuvée en mars 2023. Ainsi, en date du présent rapport, la Société répond à l'exigence et aucune action supplémentaire n'est jugée nécessaire.

[26] Ce document a été transmis au COCD par le Centre gouvernemental en cyberdéfense en septembre 2022.

OPPORTUNITÉS D'AMÉLIORATION

Afin d'améliorer la qualité de la sécurité de l'information de la Société, quelques opportunités d'amélioration ont été identifiées. Elles présentent les résultats de notre validation de certaines des obligations de la LGGRI prises individuellement et de la comparaison des pratiques de la Société aux bonnes pratiques reconnues.

OPPORTUNITÉ D'AMÉLIORATION 1 - Les travaux d'audit ont permis de constater qu'au 30 novembre 2022, la Société utilise des appareils téléphoniques fixes dont le système d'exploitation est désuet. La DVIEP encourage la Société à faire une analyse des risques liés à l'utilisation de ces appareils et à mettre en place des mesures de mitigation en attendant leur rehaussement ou leur délestage, le cas échéant.

OPPORTUNITÉ D'AMÉLIORATION 2 - La DGSI dispose d'un processus formel de gestion des risques connu des intervenants concernés. Cependant, les grandes étapes de ce processus ne sont pas consignées dans un seul et même document. La DVIEP encourage la DGSI à formaliser les grandes étapes de son processus de gestion des risques dans un document afin de préserver la mémoire organisationnelle, faciliter le transfert de connaissance et favoriser la compréhension commune du processus.

OPPORTUNITÉ D'AMÉLIORATION 3 - La DVIEP encourage la DGSI à rendre visible sur la page d'accueil de l'intranet de la Société la section présentant la marche à suivre lors de la réception de courriels malicieux, la détection de virus ou d'autres menaces, car elle n'est pas facilement accessible.

OPPORTUNITÉ D'AMÉLIORATION 4 - La DVIEP encourage la DGSI à mettre à jour sa Politique d'utilisation du courriel et des services d'Internet en fonction des changements organisationnels et de la réviser régulièrement.

OPPORTUNITÉ D'AMÉLIORATION 5 - La DVIEP encourage la DGSI à diffuser à l'ensemble de la Société l'offre de services du COCD ainsi que les fonctions de ses comités en sécurité de l'information.

CONCLUSION

Bien que plusieurs forces aient été relevées en matière de sécurité de l'information, notamment au niveau de l'environnement « Patrimoine », nous concluons que les éléments de non-conformité soulevés pourraient compromettre significativement la sécurité de l'information de la Société.

Nos travaux d'audit ont permis de constater que la Société ne répond pas à plusieurs des obligations minimales en matière de sécurité de l'information. En effet, nous avons notamment constaté, au niveau de l'environnement CASA :

- l'absence d'antivirus sur plus de la moitié des serveurs;
- l'absence d'essai de reprise complet à partir des copies de sauvegarde isolées;
- l'utilisation de divers systèmes d'exploitation désuets depuis plusieurs années qui ne sont plus supportés par des mises à jour de sécurité étendue.

Depuis février 2023, la majorité des activités de la Société sont tributaires du fonctionnement de l'environnement CASA. Advenant un incident, la combinaison de ces lacunes pourrait mener jusqu'à un arrêt complet des activités de la Société et des services offerts à la population, et ce, pour une période indéterminée. En effet, les mesures de protection de certains serveurs de l'environnement CASA sont déficientes et il pourrait être difficile, voir même impossible, d'utiliser les copies de sauvegardes prévues à cet effet, car elles ne font pas l'objet d'essai de reprise complet.

ANNEXE 1

DESCRIPTION DES NIVEAUX DE CONFORMITÉ

Généralement conforme (GC) Au 30 novembre 2022, la Société menait ses activités en conformité avec les obligations de la LGGRI et de la Directive

Partiellement conforme (PC) Au 30 novembre 2022, la Société menait ses activités en conformité partielle avec les obligations de la LGGRI et de la Directive. Les éléments de non-conformité ne compromettraient pas significativement la sécurité de l'information de la Société

Non conforme (NC) Au 30 novembre 2022, la Société ne menait pas ses activités en conformité avec les obligations de la LGGRI et de la Directive. Les éléments de non-conformité pourraient compromettre significativement la sécurité de l'information de la Société

ÉVALUATION DE LA CONFORMITÉ AUX EXIGENCES DE LA LGGRI

Obligations découlant de la LGGRI[27]	Conformité au 30 novembre 2022	
	Conclusion[28]	Référence au rapport d'audit / Commentaire
1. Gouvernance		
1.1. Création de la fonction de chef de la sécurité de l'information organisationnelle	PC	Constats 12 et 13
1.2. Avoir un organigramme qui inclut les responsables en sécurité de l'information avec les adaptations nécessaires, selon que l'organisme a son propre dirigeant de l'information ou non	NC	Constat 12
1.3. Mise en place de comités/groupes de travail appropriés de concertation en sécurité de l'information et d'un comité de crise	GC	Forces 1, 2 et 3 Opportunité d'amélioration 5
1.4. Mise en place d'un Centre opérationnel de cyberdéfense (COCD) et définition de son offre de services, ou avoir recours aux services d'un COCD	GC	Force 4 Opportunité d'amélioration 5

[27] Cette liste d'obligations est conforme à l'Annexe transmise par le MCN afin d'apporter des précisions sur la portée de l'audit.

[28] GC : Généralement conforme – PC : Partiellement conforme – NC : Non conforme – S.O. : Sans objet

Obligations découlant de la LGGRI[27]	Conformité au 30 novembre 2022	
	Conclusion[28]	Référence au rapport d'audit / Commentaire
2. Encadrement		
2.1. Adoption et mise en œuvre d'une politique et d'un cadre de gestion de la sécurité de l'information	PC	Constats 11 et 12
2.2. Mise en place d'un registre d'autorité	PC	Constat 12
2.3. Processus formel de gestion des risques de sécurité de l'information[29]	GC	Opportunité d'amélioration 2
2.4. Directive(s) interne(s) indiquant aux employés la marche à suivre lors de la réception de courriels malicieux, la détection de virus ou autres menaces	GC	Force 5 Opportunités d'amélioration 3 et 4
3. Événements de sécurité[30]		
3.1. Processus de prise en charge d'un événement de sécurité et sa déclaration sans délai, impliquant le chef de la sécurité de l'information organisationnelle, le chef délégué de la sécurité de l'information et le chef gouvernemental de la sécurité de l'information	GC	Force 6 Constat 15
3.2. Registre des événements de sécurité	GC	Force 6
4. Inventaire des actifs informationnels[31]		
4.1. Mise en place d'un inventaire des actifs informationnels	GC	Force 7

[29] La portée de l'audit s'est arrêtée à la validation de l'existence d'un processus de gestion des risques ainsi que des étapes minimales exigées par le MCN. Ainsi, aucun procédé d'audit n'a été effectué afin d'obtenir une assurance raisonnable quant à l'exactitude de la documentation supportant ce processus, l'exhaustivité des risques identifiés et l'exactitude des évaluations effectuées.

[30] La portée de l'audit s'est arrêtée à la validation de l'existence du processus de prise en charge d'un événement de sécurité, incluant sa déclaration sans délai, et du registre des événements de sécurité. Ainsi, aucun procédé d'audit n'a été effectué afin d'obtenir une assurance raisonnable quant à la mise en œuvre du processus tel que décrit, l'exhaustivité et l'exactitude des informations incluses dans le registre.

[31] La portée de l'audit s'est arrêtée à la validation de l'existence d'un inventaire des actifs informatiques de la Société et d'un processus de cueillette d'information. Ainsi, aucun procédé d'audit n'a été effectué afin d'obtenir une assurance raisonnable quant à l'exhaustivité de l'inventaire, l'exactitude des informations contenues et l'exhaustivité et l'exactitude de la documentation liée à la mise en œuvre du processus de cueillette d'information.

Obligations découlant de la LGGRI[27]	Conformité au 30 novembre 2022	
	Conclusion[28]	Référence au rapport d'audit / Commentaire
4.2. Processus de cueillette d'information visant à vérifier que les événements sont journalisés sur certains actifs technologiques de l'organisation, dont ceux déterminés par le MCN	GC	Force 8
5. Désuétude[32]		
5.1. Plan de rehaussement/délestage des systèmes d'exploitation désuets sur les serveurs	GC	
5.2. Plan de mitigation des vulnérabilités des systèmes d'exploitation désuets sur les serveurs en attendant leur rehaussement/délestage	NC	Constats 3 et 4
5.3. Plan de rehaussement/délestage des systèmes d'exploitation désuets sur les postes de travail	GC	
5.4. Plan de mitigation des vulnérabilités des systèmes d'exploitation désuets sur les postes de travail attendant leur rehaussement/délestage	GC	
5.5. Plan de mise à jour ou de remplacement des appareils mobiles pour avoir recours à des versions supportées par les manufacturiers	GC	Opportunité d'amélioration 1
5.6. Plan de mise à jour ou de remplacement des équipements de télécommunication (ex. : pare-feux, commutateurs, etc.) pour avoir recours à des versions supportées par les manufacturiers	GC	
6. Vulnérabilités[33]		
6.1. Plan de détection des vulnérabilités pour les actifs internes	GC	

[32] La portée de l'audit s'est arrêtée à la validation de l'existence des différents plans. Ainsi, aucun procédé d'audit n'a été effectué afin d'obtenir une assurance raisonnable quant à l'exhaustivité des systèmes et appareils inclus dans ces plans, l'exactitude des informations présentées et leur efficacité.

[33] La portée du présent mandat s'est arrêtée à la validation de l'existence des divers plans et stratégies en gestion des vulnérabilités. Ainsi, aucun procédé d'audit n'a été effectué afin d'obtenir une assurance raisonnable quant à l'efficacité de ces plans et stratégies ainsi qu'à l'exhaustivité et l'exactitude des informations transmises.

Obligations découlant de la LGGRI[27]	Conformité au 30 novembre 2022	
	Conclusion[28]	Référence au rapport d'audit / Commentaire
6.2. Plan d'application des correctifs sur les systèmes d'exploitation et logiciels sur les serveurs	NC	Constats 3 et 4
6.3. Plan d'application des correctifs sur les systèmes d'exploitation et logiciels sur les postes de travail	GC	
6.4. Plan d'application des correctifs, dès leur disponibilité, sur les appareils mobiles	GC	
6.5. Stratégie de mise à jour automatisée des postes de travail hors site	GC	
6.6. Stratégie de validation de la conformité des postes non gérés qui se connectent à l'infrastructure VPN	S.O.	Selon la DGSI, aucun poste non géré ne se connecte à l'infrastructure VPN de la Société
6.7. Inscription au service de balayage de vulnérabilités du Centre gouvernemental de cyberdéfense	GC	
6.8. Processus en continu pour corriger les lacunes découvertes	NC	Constat 5
6.9. Inventaires des tests d'intrusion et de vulnérabilité réalisés depuis moins d'un an	GC	
7. Reprise informatique		
7.1. Infrastructure de sauvegarde isolée pour protéger les données des attaques provenant du réseau	NC	Constat 2
7.2. Plan de reprise informatique intégrant les actifs critiques qui soutiennent les services essentiels	NC	Constat 7
7.3. Stratégie de prise de copies quotidienne	NC	Constat 2
7.4. Inventaire des exercices de recouvrement effectués périodiquement, entre autres pour valider que les copies sont fonctionnelles	NC	Constat 2
7.5. Critères et conditions pour l'activation du plan de reprise	GC	

Obligations découlant de la LGGRI[27]	Conformité au 30 novembre 2022	
	Conclusion[28]	Référence au rapport d'audit / Commentaire
7.6. Inventaire des exercices de simulation du plan de reprise informatique	NC	Constat 2
8. Confidentialité		
8.1. Preuve de la présence d'une solution de courriel sécurisé	PC	Force 9 Constat 9
9. Surveillance[34]		
9.1. Stratégie de journalisation des accès aux systèmes exposés sur Internet	GC	
9.2. Stratégie de journalisation des accès des employés aux systèmes de l'organisation	GC	
9.3. Stratégie de surveillance pour détecter et bloquer les tentatives de connexion anormales aux systèmes exposés sur Internet	GC	
10. Formation		
10.1. Inventaire des campagnes de simulation à l'hameçonnage menée de façon continue	NC	Constat 10
10.2. Plan de formation périodique en cybersécurité pour sensibiliser les employés de manière continue sur le sujet et sur les échanges de données confidentielles	GC	Forces 10 et 11
11. Gestion des identités et des accès[35]		
11.1. Processus de gestion des identités et des accès (GIA) comprenant les mécanismes d'ajout, de révision périodique et de retrait des accès pour la gestion du mouvement du personnel	GC	

[34] La portée du présent mandat s'est arrêtée à la validation de l'existence de stratégies de journalisation des accès et de surveillance. Ainsi, aucun procédé d'audit n'a été effectué afin d'obtenir une assurance raisonnable quant à l'efficacité des stratégies, l'exhaustivité et l'exactitude des journaux d'accès.

[35] La portée de l'audit s'est arrêtée à la validation de l'existence des processus et de l'inventaire, ainsi qu'à la consultation des divers rapports d'audit interne et externe en suivi. Ainsi, aucun procédé d'audit n'a été effectué afin d'obtenir une assurance raisonnable quant à la mise en œuvre de ces processus ainsi quant à l'exhaustivité et l'exactitude des informations présentées à l'inventaire.

Obligations découlant de la LGGRI[27]	Conformité au 30 novembre 2022	
	Conclusion[28]	Référence au rapport d'audit / Commentaire
11.2. Processus de GIA comprenant les mécanismes d'ajout, de révision périodique et de retrait des accès pour la gestion des privilèges élevés/administrateur	PC	Constat 6
11.3. Inventaire des mécanismes d'évaluation du processus de GIA et de présentation des résultats de l'appréciation aux autorités	GC	Force 12
12. Accès aux services gouvernementaux		
12.1. Implantation de l'authentification multifacteur (MFA) pour l'accès aux systèmes exposés sur Internet	NC	Constat 14
12.2. Implantation d'un dispositif captcha ou d'une mesure anti-robot pour l'authentification aux services externes	GC	
12.3. Mécanisme de notification avisant le citoyen des accès ou des changements à son compte	S.O.[36]	
12.4. Mécanisme permettant aux citoyens de transmettre des informations de manière sécuritaire, autre que le courriel	GC	Force 13
13. Antivirus[37]		
13.1. Preuve du déploiement sur les serveurs et les postes de travail d'un antivirus à jour	NC	Force 14 Constat 1
13.2. Preuve que l'antivirus a les fonctionnalités d'*Endpoint Detection and Response* (EDR)	NC	Force 15 Constat 1
14. Autres éléments		
Irrégularités et menaces importantes non prises en charge retracées au cours de l'audit	S.O.	Constat 8

[36] En date du 30 novembre 2022, la création d'un compte pour le citoyen n'était pas offerte par la Société

[37] La DVIEP n'a pas pu s'assurer de l'exhaustivité des serveurs et des postes de travail inclus dans les outils de gestion des antivirus. De plus, ces outils permettant une gestion en temps réel, il n'a pas été possible d'obtenir certaines informations en date du 30 novembre 2022.

ANNEXE 2

ABRÉVIATIONS

BIA	Analyse des impacts d'affaires
Bilan	Bilan de sécurité de l'information
Cadre SI	Cadre de gestion en sécurité de l'information
CAPA / CAPV	Comité actif-passif et audit (anciennement le Comité actif-passif et vérification)
CDSI	Chef délégué de la sécurité de l'information
COCD	Centre opérationnel de cyberdéfense
CSIO	Chef de la sécurité de l'information organisationnelle
CTIC	Comité des technologies de l'information et de cybersécurité
CTIC-CAPV	Comité conjoint comprenant les membres du CAPV et du CTIC
DGIT	Direction générale de l'infrastructure technologique
DGSI	Direction générale de la sécurité de l'information
Directive	Directive gouvernementale sur la sécurité de l'information
DLP	Data Loss Prevention
DVIEP	Direction de la vérification interne et de l'évaluation des programmes
EDR	Endpoint Detection and Response
GIA	Gestion des identités et des accès
LGGRI	Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, chapitre G-1.03)
MCN	Ministère de la Cybersécurité et du Numérique
Politique GIR	Politique de gestion intégrée des risques
Politique SI	Politique en sécurité de l'information
VPEN	Vice-présidence à l'expérience numérique

Société de l'assurance automobile
Québec

Avec vous,
au cœur de votre sécurité