29_P-113.1

Rapport d'audit sur le 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

Présenté au Comité actif-passif et audit

21 juin 2023

Société de l'assurance automobile Québec
Avec vous, au cœur de votre sécurité

Plan de la présentation

- Contexte
  - Mise en contexte
  - Rôles et responsabilités
  - Objectif du mandat d'audit
  - Étendue et portée du mandat d'audit
  - Limitations aux travaux d'audit
- Forces relevées
- Constats, recommandations et plan d'action
- Opportunités d'amélioration
- Conclusion
- Annexe 1 – Évaluation de la conformité aux exigences de la LGGRI

Contexte

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** (ci-après LGGRI) et de la *Directive gouvernementale sur la sécurité de l'information* (ci-après Directive) ont introduit un nouveau modèle de gouvernance en sécurité de l'information (ci-après SI) qui vise à:

- Renforcer la prise en charge des exigences de SI;
- Contrôler et vérifier les mesures afférentes;
- Assurer une réaction rapide et proactive en cas de menaces et de cyberattaques.

* Révision sanctionnée en juin 2021

Mise en contexte (suite)

La LGGRI prévoit notamment l'audit du respect des obligations en matière de SI qui en découlent.

- Le premier audit devait être réalisé au plus tard le 10 juin 2023;
- Par la suite, un audit devra être réalisé tous les cinq ans.

Rôles et responsabilités

Les responsabilités en matière de SI sont attribuées à tous les niveaux de l'organisation, incluant notamment :

- Les détenteurs d'actifs informationnels de la Société;
- L'ensemble des utilisateurs qui y accèdent, les utilisent ou les gèrent.

La SI 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 (ci-après le CSIO)

Objectifs du mandat d'audit

Le présent audit vise à s'assurer du respect de certaines obligations en matière de SI découlant de la LGGRI en date du 30 novembre 2022

Les obligations à considérer ont été préétablies par le ministère de la Cybersécurité et du Numérique (ci-après le MCN) et ont été regroupées en 13 sections.

- 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 ainsi que des bonnes pratiques en matière de SI.
- Les conclusions quant au respect des obligations par section sont présentées à l'Annexe 1

Étendue et portée du mandat d'audit

La DVIEP a procédé à l'audit du respect, au 30 novembre 2022, de certaines obligations en matière de SI 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 MCN.
- Les obligations incluses dans la portée de l'audit sont présentées à l'Annexe 1
- Elles portent sur l'ensemble du processus de gestion de la SI de la Société, de la gouvernance qui l'encadre jusqu'à sa mise en application

Étendue et portée du mandat d'audit (suite)

Les travaux d'audit ne peuvent suffire à s'assurer de l'efficacité de l'encadrement en matière de SI ni de la prise en charge adéquate et en temps opportun de l'exhaustivité des lacunes en SI.

- 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.

- Le mandat permet de conclure sur la conformité à certaines obligations en matière de SI en date du 30 novembre 2022, mais il peut également faire référence à des situations antérieures ou ultérieures au 30 novembre 2022, le cas échéant.

Étendue et portée du mandat d'audit (suite)

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.

Les procédés d'audit appliqués visaient à recueillir des éléments probants suffisants et appropriés et à les analyser pour fonder les conclusions sur les objectifs d'audit 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.

Étendue et portée du mandat d'audit (suite)

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

- Afin d'améliorer la qualité de la SI de la Société, quelques opportunités d'amélioration ont été identifiées

- Afin d'en assurer la continuité, les forces et bonnes pratiques réalisées à la Société ont aussi été identifiées

Limitations aux travaux d'audit

Délais octroyés

- Bien que le mandat d'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 la portée de l'audit n'ont été transmises à la haute direction de la Société que le 15 décembre 2022
- La DVIEP n'a été mandatée pour ce mandat qu'en février 2023
- Ainsi, les travaux de la DVIEP ont été limités dans le temps et certaines informations historiques n'ont pu être obtenues afin de conclure sur la conformité en date du 30 novembre 2022

Limitations aux travaux d'audit (suite)

Portée et étendue de l'audit

- Les précisions du MCN concernant la portée de l'audit permettaient de limiter les éléments à auditer à certaines obligations, 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 limiter ses travaux aux critères minimums prédéfinis par le MCN

Limitations aux travaux d'audit (suite)

Confidentialité des informations

- Pour des raisons de confidentialité évoquées par la direction générale de la sécurité de l'information (ci-après DGSI), plusieurs documents supportant les activités en matière de SI n'ont pas été transmis à la DVIEP.
- Certains lui ont été présentés lors de rencontres virtuelles aux fins d'observation seulement.
- Il est impossible pour un auditeur d'émettre une opinion basée seulement sur des observations. Ainsi, la DVIEP tient à informer les lecteurs que certains travaux d'audit se sont limités à la validation de l'existence des éléments à vérifier.
- La portée de l'audit de certains éléments 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 en matière de SI.

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.

Limitations aux travaux d'audit (suite)

Considérant ces limitations, 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.

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.

Les travaux d'audit se sont limités à valider 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.

Forces relevées

1. La Société bénéficie d'une direction générale dédiée à la SI. Les activités en SI sont encadrées depuis plusieurs années par un Cadre de gestion et une Politique qui définissent notamment les responsabilités essentielles en matière de SI
2. Le comité sur la SI est la principale instance de concertation en SI à la Société depuis plusieurs années
3. La Société a mis en place un comité de gestion de crise qui relève directement du président-directeur général, et ce, depuis plusieurs années. Les intervenants clés en SI sont prévus dans le plan de gestion de crise de ce comité.

Forces relevées (suite)

4. La Société a créé, en 2019, un Centre opérationnel de cyberdéfense (ci-après COCD) qui a pour mission de prévenir les cyberattaques, les traiter afin de réduire leurs impacts et assurer la continuité des services offerts aux citoyens
5. La Société met à la disposition de ses employés plusieurs directives internes indiquant la marche à suivre lors de la réception de courriels malicieux, la détection de virus ou la présence d'autres menaces
6. La documentation entourant le processus de la gestion des événements d'intérêts est effectuée de manière claire et précise par le COCD

Forces relevées (suite)

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
8. Le processus de journalisation des événements de la Société est clairement documenté et mis en œuvre
9. La Société met à la disposition de ses employés plusieurs solutions de courriels sécurisés
10. La Société bénéficie d'un plan de sensibilisation et de formation applicable à tous les intervenants de la Société

Forces relevées (suite)

11. En octobre 2022, la Société a déployé la plateforme [redacted] qui offre des autoformations mensuelles obligatoires dont le contenu permet de sensibiliser les ressources de la Société en fonction du contexte et des menaces actuels

12. En juillet 2022, la Société a déposé le dossier d'affaires *Gestion de l'identité et des mécanismes d'authentification – volet 1* visant l'amélioration de son processus de gestion des identités et des accès. À terme, ce dossier d'affaires intègrera plusieurs des recommandations déjà émises par les auditeurs internes et externes

Forces relevées (suite)

13. La Société offre à sa clientèle plusieurs mécanismes pour transmettre des informations confidentielles de façon sécuritaire
14. Les antivirus sur les postes de travail et les serveurs supportant l'environnement « Patrimoine » sont à jour et adéquatement contrôlés. Des contrôles sont en place pour suivre en temps réel l'état de conformité de ces antivirus et pour limiter l'accès aux postes de travail dont l'antivirus est obsolète
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 [redacted], mais également les fonctionnalités [redacted]

Constats, recommandations et plan d'action

Les constats et recommandations présentés visent à répondre aux objectifs de l'audit. Ils ont été préalablement validés par la DGSI

Les plans d'action soumis ont été appréciés par la DVIEP et intégrés au présent rapport.

Les constats sont présentés en fonction de la priorité des risques selon l'évaluation de la DVIEP

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

Recommandation

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

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

Constat 2

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

Recommandations

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

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

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

Constat 2 (suite)

Actions prévues 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. Il 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

* 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

Recommandations

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

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

Constat 3 (suite)

Actions prévues par la VPEN	Responsable	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		

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

Recommandations

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

Actions prévues 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

Constat 5

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

Recommandations

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

* Voir les constats 1, 3 et 4 pour le détail des vulnérabilités retracées au cours de l'audit

Constat 6

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

Recommandations

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

Constat 6 (suite)

Recommandations

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 les accès à [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

Recommandation

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*.

Actions prévues 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

* 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

Recommandation

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.

Actions prévues 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*

Recommandation

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	Responsable	Échéance
Faire des activités de sensibilisation ciblées portant sur l'échange sécuritaire de renseignements confidentiels	DGSI	2023

* 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

Recommandation

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* de la Société

Actions prévues 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.

Recommandations*

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

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

* 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 de la Société n'avaient pas été mis à jour afin de se conformer aux dernières exigences de la LGGRI et de la Directive

Constat 12 (suite)

Recommandations

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.

Constat 12 (suite)

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

Constat 13

L'attribution de la fonction de chef de la sécurité de l'information organisationnelle (ci-après CSIO) au sein de la Société ne respecte pas les exigences de la Directive

Recommandations

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

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.

Constat 13 (suite)

Actions prévues par la VPEN	Responsable	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

Cependant, depuis le 20 février 2023, les commerçants et mandataires en vérification mécanique doivent premièrement s'authentifier via le Service d'authentification gouvernementale (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

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.

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.

Opportunités d'amélioration

1. 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.
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.
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.

Opportunités 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.
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 SI notamment au niveau de l'environnement « Patrimoine », nous concluons que les éléments de non-conformité soulevés pourraient compromettre significativement la SI de la Société.

Conclusion (suite)

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 – Évaluation de la conformité aux exigences de la LGGRI

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**

La liste d'obligations présentée dans les prochaines diapositives est conforme à l'Annexe transmise par le MCN afin d'apporter des précisions sur la portée de l'audit

Évaluation de la conformité aux exigences de la LGGRI

Obligations découlant de la LGGRI	Conformité au 30 novembre 2022	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
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

Évaluation de la conformité aux exigences de la LGGRI

Obligations découlant de la LGGRI	Conformité au 30 novembre 2022	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	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

Élément 2.3 - La portée de l'audit s'est limitée 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.

Évaluation de la conformité aux exigences de la LGGRI

Obligations découlant de la LGGRI	Conformité au 30 novembre 2022	Référence au rapport d'audit / Commentaire
3. Événements de sécurité		
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

La portée de l'audit s'est limitée 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.

Évaluation de la conformité aux exigences de la LGGRI

Obligations découlant de la LGGRI	Conformité au 30 novembre 2022	Référence au rapport d'audit / Commentaire
4. Inventaire des actifs informationnels		
4.1. Mise en place d'un inventaire des actifs informationnels	GC	Force 7
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

La portée de l'audit s'est limitée 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.

Évaluation de la conformité aux exigences de la LGGRI

Obligations découlant de la LGGRI	Conformité au 30 novembre 2022	Référence au rapport d'audit / Commentaire
5. Désuétude		
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	

La portée de l'audit s'est limitée 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.

Évaluation de la conformité aux exigences de la LGGRI

Obligations découlant de la LGGRI	Conformité au 30 novembre 2022	Référence au rapport d'audit / Commentaire
5. Désuétude (suite)		
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 ([redacted]) pour avoir recours à des versions supportées par les manufacturiers	GC	

Évaluation de la conformité aux exigences de la LGGRI

Obligations découlant de la LGGRI	Conformité au 30 novembre 2022	Référence au rapport d'audit / Commentaire
6. Vulnérabilités		
6.1. Plan de détection des vulnérabilités pour les actifs internes	GC	
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	

La portée du présent mandat s'est limitée 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.

Évaluation de la conformité aux exigences de la LGGRI

Obligations découlant de la LGGRI	Conformité au 30 novembre 2022	Référence au rapport d'audit / Commentaire
6. Vulnérabilités (suite)		
6.6. Stratégie de validation de la conformité des postes non gérés qui se connectent à l'infrastructure [redacted]	S.O.	Selon la DGSI, aucun poste non géré ne se connecte à l'infrastructure [redacted] 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	

Évaluation de la conformité aux exigences de la LGGRI

Obligations découlant de la LGGRI	Conformité au 30 novembre 2022	Référence au rapport d'audit / Commentaire
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	
7.6. Inventaire des exercices de simulation du plan de reprise informatique	NC	Constat 2

Évaluation de la conformité aux exigences de la LGGRI

Obligations découlant de la LGGRI	Conformité au 30 novembre 2022	Référence au rapport d'audit / Commentaire
8. Confidentialité		
8.1. Preuve de la présence d'une solution de courriel sécurisé	PC	Force 9 Constat 9

Évaluation de la conformité aux exigences de la LGGRI

Obligations découlant de la LGGRI	Conformité au 30 novembre 2022	Référence au rapport d'audit / Commentaire
9. Surveillance		
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	

La portée du présent mandat s'est limitée 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

Évaluation de la conformité aux exigences de la LGGRI

Obligations découlant de la LGGRI	Conformité au 30 novembre 2022	Référence au rapport d'audit / Commentaire
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

Évaluation de la conformité aux exigences de la LGGRI

Obligations découlant de la LGGRI	Conformité au 30 novembre 2022	Référence au rapport d'audit / Commentaire
11. Gestion des identités et des accès		
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	
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

La portée de l'audit s'est limitée 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 spécifique 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.

Évaluation de la conformité aux exigences de la LGGRI

Obligations découlant de la LGGRI	Conformité au 30 novembre 2022	Référence au rapport d'audit / Commentaire
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.	En date du 30 novembre 2022, la création d'un pour le citoyen n'était pas offerte par la Société
12.4. Mécanisme permettant aux citoyens de transmettre des informations de manière sécuritaire, autre que le courriel	GC	Force 13

Évaluation de la conformité aux exigences de la LGGRI

Obligations découlant de la LGGRI	Conformité au 30 novembre 2022	Référence au rapport d'audit / Commentaire
13. Antivirus		
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 [redacted]	NC	Force 15 Constat 1

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.

Évaluation de la conformité aux exigences de la LGGRI

Obligations découlant de la LGGRI	Conformité au 30 novembre 2022	Référence au rapport d'audit / Commentaire
14. Autres éléments		
Irrégularités et menaces importantes non prises en charge retracées au cours de l'audit	S.O.	Constat 8