Services professionnels de vérification de l'optimisation des ressources - Gestion de crise, volet TI/cybersécurité

Rapport de vérification d'optimisation des ressources

Ville de Sept-Îles

Le 15 décembre 2023

1155, BOUL. RENÉ-LÉVESQUE O., 23E ÉTAGE, MONTRÉAL QC, H3B 2K2

T : 888.861.9724 F : 514.861.9446 MNP.ca

Table des matières

1. Sommaire de gestion

Contexte : Compte tenu de l'évolution du paysage des cybermenaces et des risques d'interruption des services informatiques pouvant compromettre la continuité des opérations de la Ville, la capacité de gérer une crise TI/Cybersécurité est une priorité pour la Ville de Sept-Îles. Ce processus a donc été retenu comme devant faire l'objet d'une vérification d'optimisation des ressources.

Objectif : L'objectif du mandat vise à valider qu'un plan de gestion de crise TI/Cybersécurité est en place, à jour, compris et adéquat. Ce mandat prévoit également une comparaison entre les pratiques de la Ville et les bonnes pratiques.

Portée : La portée du mandat couvre le processus de gestion de crise TI/cybersécurité, tel qu'exécuté par les différents services de la Ville, le cas échéant.

Période couverte : Les travaux visés par ce mandat se sont déroulés entre octobre et décembre 2023.

Exclusions : Les aspects de résilience d'affaires TI suivants ont été exclus de l'étendue du mandat :

- Continuité des activités pendant la crise.
- Plan de reprise après la crise.

Conclusion : À la suite des travaux réalisés, il est possible de constater que la Ville de Sept-Îles n'a ni formalisée, ni documentée ni implémentée de plan de gestion de crise TI/Cybersécurité et qu'elle réagit aux crises en se reposant sur les compétences de ses ressources sans plan formel structurant leurs décisions.

2. Vue d'ensemble

Ville de Sept-Îles (« Ville ») : Compte tenu de l'évolution du paysage des cybermenaces et des risques d'interruption des services informatiques pouvant compromettre la continuité des opérations de la Ville, la capacité de gérer une crise TI/Cybersécurité est une priorité pour la Ville de Sept-Îles.

Ainsi, en raison de l'augmentation généralisée des problématiques associées aux cyberattaques, il a été jugé pertinent que la Ville de Sept-Îles procède à un audit d'optimisation des ressources du processus de gestion de crise, volet TI/cybersécurité. En effet, ce processus est considéré comme essentiel au bon fonctionnement des activités de la Ville, elle désire donc s'assurer que le processus en place à cet effet est efficace et efficient.

Résilience d'affaires TI : La résilience d'affaires est la capacité d'une organisation à anticiper, à se préparer et à réagir aux perturbations soudaines. La résilience d'affaires permet de :

- Minimiser la confusion et permettre la prise de décisions efficaces en temps de crise ;
- Réduire la dépendance vis-à-vis de membres clés du personnel ou d'actifs spécifiques ;
- Minimiser la perte de données, de revenus et de clients ;
- Faciliter la reprise rapide des activités ;
- Maintenir l'image et la réputation publique de la municipalité.

La résilience d'affaires se divise en trois grands aspects :

1. Gestion de crise
2. Continuité des activités pendant la crise
3. Plan de reprise après la crise

Ce mandat se concentre sur le premier aspect, soit la gestion de crise, et plus précisément celle portant sur les TI/Cybersécurité.

Définitions : Afin d'assurer une compréhension commune de la terminologie utilisée dans ce document, certaines notions doivent être définies. Ainsi, il importe de distinguer **Incident** et **Crise**, car ces notions sont souvent confondues ou fusionnées :

- **Incident :** Évènement ou perturbation imprévu ayant des répercussions négatives, mais qui ne répond pas aux critères d'une crise. L'évènement ou la perturbation peut être géré au sein de l'équipe concernée à partir des procédures opérationnelles existantes. Généralement, les impacts d'un incident sont localisés et de courte durée.
- **Crise :** Évènement ou perturbation importante imprévu ayant des répercussions négatives majeures pour l'organisation et nécessitant une gestion spécifique pour limiter les impacts internes et externes à l'organisation et éviter ou limiter la dégradation de la situation. Généralement, une crise engendre des impacts à l'échelle de l'organisation et nécessite une coordination centralisée.

Ce mandat porte sur la gestion de crise et non sur la gestion des incidents.

3. Mandat

3.1 Objectif

L'objectif du mandat est de valider que le plan de gestion de crise portant sur les TI/Cybersécurité de la ville de Sept-Îles est en place, à jour, compris et adéquat. Ce mandat prévoit aussi une comparaison entre les pratiques de la Ville et les bonnes pratiques. À cet effet, des exemples sont présentés.

3.2 Portée/Étendue

La portée du mandat couvre le processus de gestion de crise TI/cybersécurité, tel qu'exécuté par les différents services de la Ville, le cas échéant.

Exclusions

Les aspects de résilience d'affaires TI suivants ont été exclus de l'étendue du mandat :

- Continuité des activités pendant la crise.
- Plan de reprise après la crise.

3.3 Exécution

Les travaux effectués dans le cadre de ce mandat ont été les suivants :

- Rencontrer les différents intervenants ;
- Réviser la documentation et valider si elle est cohérente avec les requis d'un plan de gestion de crise ;
- Prendre connaissance des données et des informations disponibles ;
- Proposer des pistes d'amélioration et de bonnes pratiques, le cas échéant

MNP remercie toutes les personnes qui ont participé aux travaux pour leur coopération tout au long de ce mandat.

3.4 Principaux risques

Les principaux risques associés à ce mandat sont les suivants :

- Risque lié à la continuité des activités. Absence de mesures visant à assurer le maintien des activités et des services indispensables de la Ville en cas de crise.
- Risque lié à la confidentialité des données. Absence de mesure de protection des données ou échec de ces mesures suite à une crise pour limiter l'accès et la diffusion des données aux seules personnes ou entités autorisées.
- Risque lié à l'intégrité des données. Absence de mesure de protection des données ou échec de ces mesures suite à une crise, pour garantir que les données ne subissent aucune altération accidentelle ou non autorisée lors de leur traitement, de leur transmission ou de leur conservation.
- Risque lié à la disponibilité des données. Les données ne sont pas disponibles suite à une crise.

4. Résultats

4.1 Plan de gestion de crise

Constat 1 : L'absence d'un plan formel de gestion de crise réduit la capacité de la Ville à coordonner efficacement les efforts en cas de crise et entraine un risque significatif sur la continuité des opérations de la Ville.

L'absence d'un plan formel de gestion de crise n'a pas empêché la Ville de gérer et résoudre des crises TI par le passé. Cependant, l'organisation actuelle (c.-à-d. l'absence de plan de gestion de crise TI/cybersécurité) ne favorise pas une gestion optimale des crises, considérant qu'une approche structurée et coordonnée n'a pas été définie.

Ainsi, les travaux effectués ont permis de revoir les dernières crises TI ayant affectées la Ville afin de comprendre l'approche adoptée pour leur résolution. La revue permet de faire les constats suivants :

- Aucun comité ni équipe de gestion de crise TI/cybersécurité n'est en place à Ville. Ainsi, les décisions prises lors des crises peuvent l'être manière isolée et/ou non coordonnée, sans la collaboration ou l'apport du personnel qualifié en la matière et/ou habilité à prendre des décisions, ce qui peut limiter l'efficacité des actions prises ou être contre-productif.
- Aucun responsable de la gestion de crise pour superviser les tâches de résolution de la crise et faciliter la communication entre toutes les parties n'a été désigné par la Ville.
- Aucun plan de communication général avec les employés, les citoyens et autres parties prenantes (au besoin) afin de transmettre efficacement des messages et/ou instructions lors des crises n'a été développé par la Ville.
- Aucun processus de post-mortem à la suite d'une crise n'est en place à la Ville.

Les travaux ont également permis d'identifier les éléments suivants au niveau des opérations courantes des TI qui pourraient affecter la gestion de futures crises :

- Redondance limitée en matière d'expertise Systèmes et Réseau au sein de l'équipe TI qui pourrait nuire à la résolution d'une crise en cas d'absence d'un membre clé de l'équipe.
- Absence de tests réguliers de restauration des sauvegardes pour assurer leur fiabilité et efficacité.
- Manque d'espace disque pour assurer la redondance et la disponibilité en cas de défaillance.

Il nous a aussi été indiqué qu'à la suite d'une crise TI, certains usagers ont commencé à utiliser leurs propres disques externes pour conserver des documents ou autres informations.

Recommandations

- Documenter et faire approuver par les autorités compétentes un plan de gestion de crise TI/cybersécurité formalisé. L'annexe 1 présente un exemple de structure (table des matières) de plan de gestion de crise.

  Un plan de gestion de crise formalisé comprend généralement les sections suivantes : le statut du document (par exemple : version projet, version approuvée, version adoptée), le titulaire du document, la date de la dernière revue, l'approbateur, un contexte, l'objectif du document, l'audience à qui il s'adresse et s'applique, la portée (c. à d. les processus couverts par le document, etc.), les exceptions (le cas échéant), la liste des processus à mettre en place (par exemple : reddition de comptes, suivis, exercices de simulation de crise,

Recommandations

post-mortem, etc.), les rôles, les responsabilités, son application (c. à d. conséquences d'un non-respect), la liste des versions et l'imputabilité.

- Évaluer la possibilité de formaliser et documenter, dans un guide opérationnel de résolution des crises/incidents, les étapes à suivre pour l'exécution des tâches critiques, le tout, afin, notamment, de limiter l'impact en cas d'absence de membres clés de l'équipe TI et de faciliter l'intervention de chaque membre. Rendre accessible ce document à l'ensemble de l'équipe TI.
- Évaluer la possibilité de maintenir une documentation complète sur la configuration et l'architecture des systèmes pour faciliter le dépannage et les interventions d'urgence.
- Évaluer la possibilité d'encadrer et de limiter l'utilisation des disques externes personnels pour conserver des documents ou autres informations.

Bonnes pratiques

Pratiques professionnelles pour la gestion de la continuité des activités en cas de crise : Créés et maintenus par le *Disaster Recovery Institute International* (DRI), les pratiques professionnelles pour la gestion de la continuité des activités en cas de crise sont un ensemble de connaissances conçues pour aider au développement, à la mise en œuvre et à la maintenance de programmes de continuité des activités en cas de crise.

La gestion de la continuité des activités est un processus de gestion holistique qui identifie les menaces potentielles pour une organisation et les impacts sur les opérations que ces menaces, si elles se matérialisent, pourraient engendrer. La gestion de la continuité des activités fournit un cadre pour renforcer la résilience organisationnelle avec la capacité d'une réponse efficace qui protège les intérêts des principales parties prenantes, la réputation, la marque et les activités créatrices de valeur.

En résumé, les pratiques professionnelles pour la gestion de la continuité des activités visent à :

- **Gestion du programme** : Établir la nécessité d'un programme de continuité des activités, et présenter les concepts clés (gestion de programme, sensibilisation aux risques, impact sur les fonctions/processus critiques, stratégies de récupération, formation, sensibilisation, ainsi qu'exercices/tests).
- **Évaluation des risques** : Identifier les risques qui pourraient avoir un impact sur les ressources, les processus ou la réputation d'une entité et les évaluer pour déterminer les impacts potentiels sur la municipalité, permettant à l'entité de déterminer les moyens les plus efficaces pour les réduire.
- **Analyse de l'impact sur les entreprises** : Identifier et hiérarchiser toutes les fonctions, processus et dépendances de la municipalité afin de déterminer ceux ayant le plus grand impact en cas d'indisponibilité. Analyser, documenter et communiquer les résultats pour mettre en évidence tous les écarts entre les exigences de la municipalité et ses capacités actuelles.
- **Stratégies de continuité des activités** : Sélectionner des stratégies pour réduire les écarts identifiés lors de l'évaluation des risques et de l'analyse de l'impact sur les activités.
- **Préparation et réponse aux incidents** : Comprendre les types d'incidents qui pourraient menacer la vie, les biens, les opérations ou l'environnement, leurs impacts potentiels et établir et maintenir des capacités de protection. Mise en œuvre d'un système de gestion des incidents pour commander, contrôler et

coordonner les activités de réponse, de continuité et de récupération avec des ressources internes et externes.

- **Élaboration et mise en œuvre du plan** : Documenter les plans à utiliser lors d'un incident qui permettront à l'entité de continuer à fonctionner et définir les critères d'exercice/de test pour valider que les plans atteindront l'objectif souhaité.
- **Programmes de sensibilisation et de formation** : Établir et maintenir des programmes de formation et de sensibilisation permettant au personnel d'être capable de réagir aux incidents perturbateurs de manière calme et efficace.
- **Exercice/test, évaluation et maintenance du plan de continuité des activités** : Établir un programme d'exercices/tests, d'évaluation et de maintenance du plan de continuité des activités pour maintenir un état de préparation de l'entité.
- **Communications de crise** : Créer et maintenir un plan de communication de crise. Veiller à ce que le plan de communication de crise prévoit une communication rapide et efficace avec les parties internes et externes.
- **Coordination avec les agences et ressources externes** : Établir des politiques et des procédures pour coordonner les activités d'intervention avec les entités publiques et les ressources privées concernées, conformément à la cinquième pratique professionnelle : préparation et réponse aux incidents.

Constat 2 : L'équipe TI n'organise pas de tests ni d'exercice de simulation de crise. L'absence de tests et d'exercice de simulation de crise réduit la capacité de l'équipe TI à gérer efficacement les crises.

Recommandations

- Une fois la mise en place d'un plan formel de gestion de crise, instaurer une routine de tests réguliers du plan et/ou d'exercice de simulation de crise pour confirmer l'efficacité du plan et celle de l'équipe, et valider la pertinence du plan face aux évolutions des menaces et des technologies.
- Après chaque test et/ou simulation, évaluer la performance de la Ville en gestion de crise et apporter les ajustements nécessaires pour améliorer continuellement les procédures de gestion de crise.
- Organiser des test et/ou des simulations de crise en incluant des scénarios où la personne clé dans le domaine affecté est absente afin d'identifier et de combler les lacunes, le cas échéant, dans les procédures de gestion de crise.

Constat 3 : Lors des crises TI passées, aucune réunion de post-mortem n'a été réalisée pour analyser l'approche de gestion de crise et identifier des points d'amélioration. Une absence de post-mortem documenté rend la Ville vulnérable à des défaillances répétées et réduit sa capacité d'amélioration continue.

Recommandations

- Mettre en place un processus formalisé de post-mortem après chaque crise pour analyser les causes de la crise, les actions réalisées, les points forts de la réponse et les points d'améliorations. Mettre en place des plans d'action pour adresser les points d'améliorations identifiés.

4.2 Reddition de comptes

Constat 4 : La Ville n'a pas défini de requis de reddition de comptes à la suite d'une crise TI/Cybersécurité. L'absence d'un système structuré de reddition de comptes limite les capacités de la Ville à évaluer et à améliorer sa gestion de crise TI/Cybersécurité. La reddition de comptes permet de rendre compte de manière transparente des performances et des défis liés à la gestion de crise.

Recommandations

- Mettre en place un système de reddition de comptes pour informer les autorités compétentes sur, notamment, :
  - la crise, sa gravité, ses impacts ;
  - certains indicateurs liés à la gestion de crise, comme la durée moyenne d'une crise, le temps moyen d'activation de la cellule de crise, le temps moyen de récupération, etc. ;
  - l'avancement des plans d'action suite aux post mortem ;
  - la perception des citoyens, employés, et autres parties prenantes, au besoin sur la gestion de crise.

5. Conclusion

À la suite des travaux réalisés, il est possible de constater que la Ville de Sept-Îles n'a ni formalisé, ni documentée ni implémentée de plan de gestion de crise TI/Cybersécurité et qu'elle réagit aux crises en se reposant sur les compétences de ses ressources sans plan formel structurant leurs décisions.

Annexe 1 :
Exemple de tables des matières - Plan de gestion de crise

Annexe 2 :
Critères d'audit

Les critères se concentrent sur les résultats que l'on souhaite obtenir du processus, du programme, de l'opération, du système ou du contrôle. Les observations découlent de l'évaluation selon laquelle les critères sont respectés ou non.

Pour ce mandat, les critères suivants ont été évalués.

1. La Ville s'est dotée d'un plan de gestion de crise TI/cybersécurité qui lui permet de réagir adéquatement en tant de crises. Ce plan :
    1.1. est complet ;
    1.2. permet aux équipes de prendre action en temps opportun ;
    1.3. est testé régulièrement ;
    1.4. permet d'identifier les points d'amélioration.
2. Une reddition de comptes périodique est faite aux autorités de la Ville à cet effet.

PRAXITY™
Empowering Business Globally

KINCENTRIC
Employeur de Choix
CANADA 2019

Partout où mènent les affaires

MNP.ca