Gestion des systèmes de contrôle industriels du métro

Société de transport de Montréal

3.6.

Le 31 janvier 2023

Rapport annuel 2022

Bureau du vérificateur général
de la Ville de Montréal

Gestion des systèmes de contrôle industriels

Mise en contexte

La Société de transport de Montréal (STM) fournit à la population de l'île de Montréal des services de transport collectif, dont le service de métro, d'autobus et de transport adapté.

En ce qui concerne le réseau du métro, il comprend 4 lignes desservant 68 stations sur 71 kilomètres. Ceci représente une offre de service de 85,3 millions de kilomètres parcourus annuellement. Le métro est contrôlé de manière centralisée par un Système de contrôle et d'acquisition de données « *Supervisory Control and Data Acquisition* » (SCADA) qui surveille et gère les opérations du métro. Cette gestion nécessite l'utilisation de systèmes de contrôle industriels (SCI) composés de technologies opérationnelles (TO) et de technologies de l'information (TI).

Les SCI, tout comme les systèmes informatiques traditionnels, peuvent être confrontés à des menaces émergentes sous la forme de cyberattaques provoquant des dommages, du vol d'information et de la destruction ou l'altération du bon fonctionnement des SCI du métro.

Le présent rapport traite de nos constatations qui sont de nature publique. Un rapport détaillé distinct a été publié uniquement à l'interne en raison des renseignements hautement sensibles et confidentiels qu'il contient.

Objectif de l'audit

Déterminer si les mécanismes mis en place à la STM permettent une saine gestion ainsi qu'une haute disponibilité des systèmes de contrôle industriels utilisés par le métro.

Résultats

Nous concluons que la gestion des SCI par la Société de transport de Montréal (STM) nécessite des améliorations afin d'assurer une gestion plus efficace et de réduire les risques de perte de disponibilité du métro.

En effet, la gestion inadéquate des accès logiques aux SCI augmente le risque d'accès non autorisés, ce qui pourrait altérer le fonctionnement du métro. De plus, l'absence de plan de relève informatique formel engendre un risque de perte de disponibilité des SCI.

Plusieurs autres éléments doivent être améliorés notamment sur le plan de :

- la formalisation des rôles et responsabilités;
- l'absence de programme de sensibilisation spécifique aux SCI du métro;
- la surveillance des systèmes;
- l'exhaustivité du processus de gestion des changements.

Toutefois, la STM dispose des mécanismes de contrôle adéquats suivants :

- Les ressources humaines de la Division Livraison des services technologiques métro sont suffisantes;
- L'architecture TI/TO est documentée avec une segmentation adéquate des réseaux;
- Les pare-feu sont mis à jour régulièrement.

Principaux constats

Rôles et responsabilités

→ Il n'existe pas de document formel détaillant le partage des rôles et responsabilités afférent aux Systèmes de contrôle industriels du métro.

Suffisance et adéquation des ressources humaines

→ Les ressources humaines en place de la Division Livraison des services technologiques métro sont suffisantes pour répondre à ses besoins.

→ Il n'existe pas de programme de sensibilisation spécifique aux SCI du métro pour les ressources de la Division Livraison des services technologiques métro.

Gestion des accès logiques

→ Les encadrements de gestion des accès logiques ne sont pas adaptés aux SCI du métro ni appliqués systématiquement.

Sécurité des réseaux liés aux environnements industriels

→ L'architecture technologique est documentée et comporte une segmentation adéquate des réseaux.

→ Les pare-feu sont mis à jour régulièrement.

→ Il n'existe pas de procédure formelle d'évaluation et d'installation des mises à jour sur les serveurs SCI.

Surveillance des systèmes

→ Un outil de surveillance et d'alerte d'événements de sécurité est en place. Toutefois, il n'existe pas d'encadrement de surveillance pour les SCI du métro.

Gestion des changements

→ Un processus formel de gestion des changements est appliqué. Cependant, celui-ci est incomplet par rapport aux saines pratiques de l'industrie.

Relève informatique des systèmes

→ Il n'existe pas de plan de relève formel des systèmes informatiques.

En marge de ces résultats, nous avons formulé différentes recommandations aux unités d'affaires qui sont présentées aux pages suivantes.

Liste des sigles

COS
centre d'opérations de sécurité

RACI
Réalisateur, Approbateur, Consulté, Informé

SCADA
Système de contrôle et d'acquisition de données « *Supervisory Control and Data Acquisition* »

SCI
systèmes de contrôle industriels

TI
technologies de l'information

TO
technologies opérationnelles

Table des matières

1. Contexte

La Société de transport de Montréal (STM) offre à la population de l'île de Montréal des services de transport collectif, dont les réseaux de métro et d'autobus et le transport adapté.

En ce qui concerne le réseau de métro, il compte 4 lignes desservant 68 stations sur 71 kilomètres de tunnel souterrain. Ceci représente une offre de service de 85,3 millions de kilomètres parcourus annuellement. En 2022, un budget de 338 M$ a été alloué au service de métro.

Le métro est contrôlé de manière centralisée par un Système de contrôle et d'acquisition de données « *Supervisory Control and Data Acquisition* » (SCADA) qui surveille et gère les opérations du métro. Cette gestion nécessite l'utilisation de systèmes de contrôle industriels (SCI) composés de technologies opérationnelles (TO) et de technologies de l'information (TI) qui ont pour principaux objectifs de :

- Réduire les risques d'indisponibilité des SCI et d'erreurs humaines en automatisant les processus;
- Accélérer les réactions aux incidents (p. ex. bris d'équipements, panne informatique) en ayant les informations en temps réel et les outils de surveillance adéquats;
- Augmenter la satisfaction de la clientèle en apportant rapidement des améliorations aux infrastructures et aux applications.

Il y a deux parties prenantes dans la gestion des SCI et qui relèvent de la Direction exécutive des technologies de l'information et de l'innovation de la STM :

- La Division Livraison des services technologiques métro concerne les aspects liés au développement, à l'exploitation, à la gestion du changement et aux infrastructures technologiques;
- La Direction Sécurité des actifs informationnels est responsable de l'aspect cybersécurité qui inclut aussi la surveillance et la gestion des incidents ainsi que la sensibilisation des membres du personnel.

Les menaces qui peuvent affecter la disponibilité du service offert aux usagers proviennent notamment :

- D'erreurs humaines ou de bris d'équipements rendant indisponible le service du métro;
- Des cyberattaques (p. ex. un rançongiciel) provoquant des dommages, du vol d'information, la destruction ou l'altération du bon fonctionnement des SCI du métro.

Actuellement, tout type de SCI (p. ex. le transport en commun, le traitement de l'eau potable, la distribution électrique) peut être confronté à ces menaces. Il est donc important de s'assurer que des mesures de contrôle des SCI sont en place afin d'en réduire les risques.

2. Objectif de l'audit, critères d'évaluation et portée des travaux

2.1. Objectif

En vertu des dispositions de la *Loi sur les cités et villes*, nous avons réalisé une mission d'audit de performance portant sur la Gestion des systèmes de contrôle industriels du métro. Nous avons réalisé cette mission conformément à la *Norme canadienne de missions de certification* (NCMC) 3001 du *Manuel de CPA Canada – Certification*.

Cet audit avait pour objectif de déterminer si les mécanismes mis en place à la STM permettent une saine gestion ainsi qu'une haute disponibilité des systèmes de contrôle industriels utilisés par le métro.

2.2. Critères d'évaluation

Notre évaluation est basée sur les critères que nous avons jugés valables dans les circonstances, soit :

1. Rôles et responsabilités

Les rôles et responsabilités des parties prenantes impliquées dans les systèmes de contrôle industriels utilisés par la STM pour le métro sont formellement documentés, complets, à jour, diffusés auprès des parties prenantes et mis en application par ces dernières.

2. Suffisance et adéquation des ressources humaines

Des ressources humaines suffisantes et adéquates sont présentes afin de concevoir et de mettre en application les saines pratiques en matière de développement, d'exploitation et de sécurité des SCI utilisés par la STM pour le métro.

3. Gestion des accès logiques

La gestion des accès logiques liés aux principaux SCI utilisés par le métro respecte les saines pratiques.

4. Sécurité des réseaux liés aux environnements industriels

L'architecture et la configuration des réseaux utilisés pour les SCI respectent les saines pratiques en matière de sécurité.

5. Surveillance des systèmes

Les principaux SCI du métro font l'objet d'une surveillance continue afin de détecter en temps opportun diverses menaces pouvant affecter le service à la clientèle du métro.

6. Gestion des changements

Le processus de gestion des changements des SCI (équipements et logiciels) du métro respecte les saines pratiques et il est systématiquement mis en application.

7. Relève informatique des systèmes

Le processus de relève des SCI du métro est documenté et testé régulièrement et prévoit des solutions en cas d'incident majeur (p.ex. sinistre forçant l'évacuation du bâtiment tel qu'un incendie).

La responsabilité de la vérificatrice générale de la Ville consiste à fournir une conclusion sur l'objectif de l'audit. Pour ce faire, nous avons recueilli des éléments probants suffisants et appropriés pour fonder notre conclusion et pour obtenir un niveau d'assurance raisonnable.

À la fin de nos travaux, un projet de rapport d'audit a été présenté, aux fins de discussions, aux gestionnaires concernés des unités d'affaires auditées. Par la suite, le rapport final a été transmis à la direction des unités d'affaires concernées ainsi qu'à la Direction de la STM.

La vérificatrice générale de la Ville applique la Norme canadienne de gestion de la qualité 1, *Gestion de la qualité par les cabinets qui réalisent des audits ou des examens d'états financiers, ou d'autres missions de certification ou de services connexes*. Cette norme exige de la vérificatrice générale de la Ville qu'elle conçoive, mette en place et fasse fonctionner un système de gestion de la qualité qui comprend des politiques et des procédures en ce qui concerne la conformité aux règles de déontologie, aux normes professionnelles et aux exigences légales et réglementaires applicables. Au cours de ses travaux, la vérificatrice générale de la Ville s'est conformée aux règles sur l'indépendance et aux autres règles de déontologie du Code de déontologie des comptables professionnels agréés du Québec, lesquelles reposent sur les principes fondamentaux d'intégrité, de compétence professionnelle et de diligence, de confidentialité et de conduite professionnelle.

Nos travaux d'audit ont porté sur la période s'échelonnant de septembre 2021 à novembre 2022. Ils ont consisté à effectuer des entrevues auprès du personnel, à examiner divers documents et à réaliser les sondages que nous avons jugés appropriés en vue d'obtenir l'information probante nécessaire. Nous avons toutefois tenu compte d'informations qui nous ont été transmises jusqu'au 31 janvier 2023.

2.3. Portée

Nos travaux ont porté sur le SCADA ainsi que les systèmes informatiques qui sont utilisés pour la planification, la gestion, le suivi et le contrôle des SCI du métro.

Ces systèmes comportent également des équipements réseau, des serveurs informatiques, ainsi que des systèmes d'exploitation.

Le présent rapport traite de nos constatations qui sont de nature publique. Un rapport détaillé distinct a été publié uniquement à l'interne en raison des renseignements hautement sensibles et confidentiels qu'il contient.

3. Résultats de l'audit

3.1. Rôles et responsabilités

Afin d'assurer une saine gouvernance et gestion des SCI utilisés par le métro, il est important d'avoir une documentation formelle, claire et détaillée des rôles et des responsabilités des différentes parties prenantes impliquées. Une telle documentation peut prendre la forme d'une matrice des rôles et des responsabilités (p. ex. un RACI (Réalisateur, Approbateur, Consulté, Informé)) approuvée, diffusée auprès des parties prenantes.

Globalement, il y a deux secteurs au sein de la Direction exécutive des technologies de l'information et de l'innovation à la STM qui sont parties prenantes sur les SCI du métro :

- Division Livraison des services technologiques métro : responsable de l'exploitation des SCI comme le SCADA dont la division est propriétaire;
- Direction Sécurité des actifs informationnels : responsable de la cybersécurité, ce qui inclut la surveillance et la gestion de la cybersécurité, la gestion des incidents et la sensibilisation.

Bien que les rôles semblent connus de tous, il n'existe pas de document formel (par exemple un RACI) détaillant le partage des rôles et responsabilités relatif aux SCI du métro pour la STM.

Il existe cependant certains documents détaillant les rôles et les responsabilités dans la Division Livraison des services technologiques métro, notamment pour les secteurs de l'automatisation, de l'intégration, de la surveillance et contrôle ainsi que du trafic et des communications. Or ces documents constituent seulement des descriptifs de postes comprenant les tâches et responsabilités et ne représentent pas à proprement dit un RACI formel.

Quant à la Direction Sécurité des actifs informationnels, elle a fait l'objet d'une réorganisation au premier trimestre de 2022. Les ressources globales de la STM en cybersécurité ont presque triplé, en plus de l'embauche d'un nouveau directeur à la Direction Sécurité des actifs informationnels. Étant donné ces changements récents, aucun RACI n'est encore documenté.

L'absence d'une telle documentation augmente le risque que des activités importantes soient omises, exécutées de façon inadéquate, ou effectuées par des intervenantes et intervenants inappropriés. La matérialisation de ces risques pourrait ultimement mener à une perte d'efficacité des opérations du métro.

RECOMMANDATION 3.1.A.

Nous recommandons à la Division Livraison des services technologiques métro et à la Direction Sécurité des actifs informationnels de :

- créer un document formel qui représente de façon détaillée le partage des rôles et des responsabilités entre la Division Livraison des services technologiques métro et la Direction Sécurité des actifs informationnels;
- s'assurer de la diffusion, de la bonne compréhension et de la mise en application de ces rôles et responsabilités auprès des parties prenantes.

3.2. Suffisance et adéquation des ressources humaines

Le maintien de ressources humaines qualifiées, expérimentées et en nombre suffisant, est essentiel afin de permettre à la STM d'atteindre ses objectifs en matière d'exploitation du métro.

Lors de nos travaux, nous avons constaté les éléments suivants dans les unités d'affaires qui sont parties prenantes dans la gestion des systèmes de contrôle industriels du métro :

- **Ressources de la Division Livraison des services technologiques métro**

  Selon les documents de gestion de capacité qui nous ont été présentés, les ressources en place (p. ex. les ingénieurs en automatisation, les architectes de réseau, les opérateurs), sont suffisantes pour répondre aux besoins des opérations ainsi que des projets relatifs aux SCI du métro. En effet, aucun élément d'information ne nous permet de détecter d'enjeux significatifs à ce niveau.

- **Ressources de la Direction Sécurité des actifs informationnels**

  Nous avons constaté l'absence de programme de sensibilisation spécifique aux SCI du métro pour les ressources de la Division Livraison des services technologiques métro. Par conséquent, les connaissances du personnel pourraient ne pas être à jour à propos des menaces pouvant affecter les SCI.

RECOMMANDATION 3.2.A.

Nous recommandons à la Direction Sécurité des actifs informationnels de développer et de mettre en place un plan de sensibilisation spécifique aux systèmes de contrôle industriels pour les ressources de la Division Livraison des services technologiques métro.

3.3. Gestion des accès logiques

La gestion des accès logiques est un contrôle de première importance en matière de sécurité de l'information. Elle permet notamment de s'assurer que seules les personnes autorisées accèdent aux systèmes d'une organisation avec les accès limités à ce qu'elles ont besoin pour leur travail.

À la suite de nos travaux d'audit, nous avons constaté les lacunes suivantes :

- Bien qu'il existe des encadrements de gestion des accès logiques à la STM, aucun n'est adapté à la réalité des SCI du métro (incluant l'octroi, la suppression, la modification, la révision des accès et l'accès à distance);
- Contrairement à la procédure de la STM, les demandes d'accès ne sont pas formelles pour un des systèmes du métro;
- Pour l'accès à la salle des serveurs du métro, nous n'avons pas pu obtenir les documents de révision des accès. Ainsi nous n'avons pas la certitude que cette vérification est réalisée.

Des encadrements non adaptés et non appliqués systématiquement pourraient augmenter le risque d'accès non autorisés à des SCI.

RECOMMANDATION 3.3.A.

Nous recommandons à la Division Livraison des services technologiques métro d'adapter les encadrements liés à la gestion des accès logiques de la STM à la réalité des systèmes de contrôle industriels du métro.

RECOMMANDATION 3.3.B.

Nous recommandons à la Division Livraison des services technologiques métro de mettre en place un processus récurrent de révision des accès à la salle des serveurs du métro et de conserver les documents afférents.

3.4. Sécurité des réseaux liés aux environnements industriels

Les réseaux du métro sont composés d'équipements (p. ex. les automates[1], les serveurs, les pare-feu[2]) reliés entre eux par des connexions (filaire, sans-fil, radio) et de protocoles de communication afin de permettre l'échange d'informations. La sécurité des réseaux consiste à mettre en place un processus pour protéger leurs composants contre les intrusions non autorisées, les modifications ou les divulgations inappropriées, et ce, afin de maintenir leur bon fonctionnement.

---

1 Automate : Machine qui exécute des tâches de façon automatique, sans intervention humaine.

2 Pare-feu : Système de sécurité conçu pour filtrer les flux de données entre un réseau et un autre réseau.

Lors de nos travaux d'audit, nous avons relevé les éléments positifs suivants :

- Une architecture réseau a été schématisée sous la forme de plusieurs documents. Les documents ont été dûment approuvés;
- Le réseau du métro est adéquatement segmenté par des réseaux virtuels. De plus, ces derniers sont isolés du réseau corporatif et d'Internet. Cette segmentation respecte les saines pratiques en matière de sécurité des réseaux;
- Les pare-feu sont mis à jour régulièrement pour protéger les équipements réseau et les serveurs applicatifs;
- D'une part, les serveurs ne sont pas accessibles à partir d'Internet et, d'autre part, ils ne peuvent également pas atteindre Internet.

Cependant, nous avons noté qu'il n'existe pas de procédure formelle d'évaluation et d'installation des mises à jour sur les serveurs SCI. Ceci augmente le risque que des mises à jour importantes ne soient pas installées ce qui pourrait impacter la disponibilité des SCI du métro.

RECOMMANDATION 3.4.A.

Nous recommandons à la Division Livraison des services technologiques métro de mettre en place une procédure formelle d'évaluation et d'installation des mises à jour.

3.5. Surveillance des systèmes

La surveillance est une activité informatique qui permet la supervision continue des systèmes informatiques. Cette surveillance se fait généralement par des logiciels spécialisés qui permettent aux administratrices et administrateurs de superviser leurs systèmes et de mesurer continuellement, entre autres, les accès non autorisés et les tentatives d'intrusions. Nous avons constaté que :

- Un outil de surveillance d'événements de sécurité est en place depuis avril 2022;
- Une ressource est dédiée à l'analyse de ces événements de sécurité;
- Advenant un événement, une alerte est envoyée à une ressource de garde de l'équipe du Centre d'opérations de sécurité (COS) de la STM.

Cependant, nous avons relevé qu'il n'existe pas d'encadrement formel lié à la surveillance des SCI du métro. Ceci augmente le risque que des activités afférentes soient réalisées de façon non homogène et non efficace.

RECOMMANDATION 3.5.A.

Nous recommandons à la Direction Sécurité des actifs informationnels en collaboration avec la Division Livraison des services technologiques métro de développer et mettre en place les encadrements formels nécessaires à une saine gouvernance de l'activité de surveillance pour les systèmes de contrôle industriels du métro.

3.6. Gestion des changements

La gestion des changements a pour objectif de s'assurer que toute modification dans un environnement de production[3] est enregistrée, évaluée, autorisée, priorisée, planifiée, testée et mise en œuvre de manière contrôlée en suivant des encadrements formellement documentés, approuvés, à jour, diffusés et respectés par les parties prenantes. C'est un élément fondamental de la gestion des risques des SCI.

Lors de nos travaux, nous avons constaté que pour les SCI du métro un processus formel de gestion des changements est documenté, à jour et connu par les parties prenantes. Cependant, celui-ci est incomplet par rapport aux saines pratiques de l'industrie.

L'équipe de l'assurance qualité est au courant de tous les changements à apporter à l'environnement de contrôle. Il y a des rencontres hebdomadaires de suivi des planifications où les changements sont présentés.

Notre analyse de la documentation pour quatre changements nous a permis de constater qu'ils suivent les exigences du processus de gestion de changement de la STM.

Avec un processus de gestion des changements incomplet, la STM pourrait s'exposer à des risques impactant la disponibilité des SCI du métro et l'intégrité et la confidentialité de leurs données.

RECOMMANDATION 3.6.A.

Nous recommandons à la Division Livraison des services technologiques métro en collaboration avec la Direction Sécurité des actifs informationnels de compléter le processus de gestion des changements afin qu'il respecte les saines pratiques de l'industrie.

3.7. Relève informatique des systèmes

Le fonctionnement du métro dépend fortement des SCI. Il est donc primordial pour la STM de se préparer à toute éventualité de sinistre pouvant perturber ou causer un arrêt de ces SCI. Les menaces peuvent survenir de l'externe comme une cyberattaque ou encore de l'interne, p. ex. un sabotage d'équipement, une défaillance technique majeure ou un bris d'équipement. Le processus comprend, entre autres, un programme de tests sur plusieurs années incluant des exercices de relève et des procédures des tests ainsi que des solutions en cas d'incident.

---

3 L'environnement de production est un terme utilisé pour décrire le cadre dans lequel les logiciels sont réellement mis en service pour leurs utilisations finales prévues.

Bien que des tests de relève aient été réalisés pour l'ensemble des SCI du métro, ceux-ci n'ont pas été effectués de façon régulière depuis 2019. Nous avons aussi constaté qu'il n'existe pas de plan de relève formel.

L'absence d'un plan de relève informatique formel ne permettrait pas à la STM d'être suffisamment préparée advenant un sinistre, ce qui pourrait conduire à un arrêt du service du métro et augmenter le délai de reprise des opérations.

RECOMMANDATION 3.7.A.

Nous recommandons à la Direction Sécurité des actifs informationnels de mettre en place un plan formel de relève informatique pour les systèmes de contrôle industriels du métro.

4. Conclusion

La gestion des systèmes de contrôle industriels (SCI) du métro par la Société de transport de Montréal (STM) nécessite des améliorations afin d'assurer une gestion plus efficace et ainsi réduire les risques potentiels de perte de disponibilité du métro.

En effet, la gestion inadéquate des accès logiques aux SCI augmente le risque d'accès non autorisés. De plus, l'absence de plan de relève informatique formel engendre un risque de perte de disponibilité des SCI.

Plusieurs autres éléments doivent être également améliorés sur le plan de :

- la formalisation des rôles et responsabilités;
- l'absence de programme de sensibilisation spécifique aux SCI du métro;
- la surveillance des systèmes;
- l'exhaustivité du processus de gestion des changements.

Toutefois, la STM dispose des mécanismes de contrôle adéquats suivants :

- Les ressources humaines en place de la Division Livraison des services technologiques métro sont suffisantes pour répondre à leurs besoins;
- L'architecture technologique est documentée et comporte une segmentation adéquate des réseaux;
- Les pare-feu sont mis à jour régulièrement;
- Un outil technologique de surveillance et d'alerte est utilisé;
- Il existe un processus formel de gestion des changements qui est appliqué et suivi.

Voici les détails selon les critères d'évaluation suivants :

Rôles et responsabilités

Bien que les rôles et responsabilités soient connus de tous, l'absence d'un document formel qui présente les parties prenantes dans la gestion des SCI du métro augmente le risque que des activités importantes soient omises, effectuées par des intervenants inappropriés ou exécutées de façon inadéquate. La matérialisation de ces risques pourrait ultimement mener à une perte d'efficacité des opérations du métro.

Suffisance et adéquation des ressources humaines

Les ressources humaines de la Division Livraison des services technologiques métro sont suffisantes. Cependant, il n'y a pas de programme de sensibilisation spécifique aux SCI du métro pour ces ressources. Par conséquent, les connaissances du personnel pourraient ne pas être à jour à propos des menaces pouvant affecter les SCI.

Gestion des accès logiques

Les encadrements de gestion des accès logiques ne sont pas adaptés aux SCI du métro ni appliqués systématiquement. Ceci peut augmenter le risque d'accès non autorisés aux SCI du métro.

Sécurité des réseaux liés aux environnements industriels

L'architecture technologique est documentée et le réseau du métro est adéquatement segmenté par des réseaux virtuels en plus d'être isolé du réseau corporatif et d'Internet. Par contre, il n'existe pas de procédure formelle d'évaluation et d'installation des mises à jour sur les serveurs SCI. Ceci augmente le risque que des mises à jour importantes ne soient pas installées, ce qui pourrait impacter la disponibilité des SCI du métro.

Surveillance des systèmes

Un outil de surveillance d'événements de sécurité est en place, mais il n'existe pas d'encadrement de surveillance pour l'ensemble des SCI du métro, ce qui augmente le risque que des activités afférentes soient réalisées de façon non homogène et non efficace.

Gestion des changements

Un processus formel de gestion des changements est appliqué. Cependant, celui-ci est incomplet par rapport aux saines pratiques de l'industrie, ce qui pourrait exposer la STM à des risques impactant la disponibilité des SCI du métro et l'intégrité et la confidentialité de leurs données.

Relève informatique des systèmes

Il n'existe pas de plan de relève informatique ce qui ne permettrait pas à la STM d'être suffisamment préparée advenant un sinistre. Cette situation pourrait conduire à un arrêt du service du métro et augmenter le délai de reprise des opérations.