Rapport du Vérificateur général du Québec
à l'Assemblée nationale pour l'année 2018-2019

Mai 2018

CHAPITRE

5

Audit de performance

Reprise informatique

Centre de services partagés du Québec
Ministère du Travail, de l'Emploi et de la Solidarité sociale
Secrétariat du Conseil du trésor

Faits saillants

Objectifs des travaux

Les ministères et organismes doivent élaborer un plan de reprise informatique pour chacun des systèmes d'information qu'ils considèrent comme essentiels à la réalisation de leur mission, et ce, afin de pouvoir les rétablir dans un délai acceptable en cas de sinistre.

Nos travaux visaient à nous assurer que :

- le ministère du Travail, de l'Emploi et de la Solidarité sociale (MTESS) et le Centre de services partagés du Québec (CSPQ) prennent les mesures nécessaires pour répondre aux risques d'interruption de service pouvant affecter la disponibilité des systèmes d'information que le MTESS juge critiques ;
- le Secrétariat du Conseil du trésor (SCT) apporte un encadrement et un soutien appropriés en matière de reprise informatique aux ministères et organismes assujettis à la *Loi sur l'administration publique*.

Le rapport entier est disponible au www.vgq.qc.ca.

Résultats de l'audit

Nous présentons ci-dessous les principaux constats que nous avons faits lors de l'audit concernant la reprise informatique.

Le MTESS n'a pas réalisé d'analyse complète de l'impact et des risques liés à la non-disponibilité de ses systèmes d'information et à leurs interdépendances. Cette analyse lui aurait permis de recenser ses systèmes d'information critiques et de déterminer, pour ceux-ci, des objectifs et des priorités en matière de reprise. Ainsi, pour l'ensemble de ces systèmes, le ministère n'est pas en mesure de conclure que les plans de reprise informatique permettraient le rétablissement de tous ses services essentiels en cas de sinistre.

Certains des systèmes appuyant les services essentiels ne font pas l'objet d'un plan de reprise informatique. Toutefois, dans les cas où un plan de reprise a été produit, celui-ci est généralement complet.

Depuis 2014-2015, la moitié des essais portant sur le plan de reprise informatique relatif à la plateforme centrale a été annulée. Quant au Régime québécois d'assurance parentale, l'objectif de rétablir ce système dans un délai de 24 heures a été atteint cinq fois sur huit.

La haute direction du MTESS n'effectue pas de suivi des plans de reprise informatique. Les décisions, comme celles portant sur les stratégies de reprise et sur les objectifs liés aux délais de reprise, n'ont pas fait l'objet de discussions au comité exécutif du ministère.

Les documents d'encadrement du SCT ne sont pas assez précis quant à l'importance et au rôle des plans de reprise informatique à l'intérieur d'un processus global de gestion de la continuité des services. Les plans de reprise informatique ne peuvent être élaborés de façon isolée. Ils doivent tenir compte de l'analyse d'impact et faire partie d'un processus global de gestion de la continuité des services.

Recommandations

Le Vérificateur général a formulé des recommandations à l'intention du MTESS, du CSPQ et du SCT. Celles-ci sont présentées intégralement ci-contre.

Les entités auditées ont eu l'occasion de transmettre leurs commentaires, qui sont reproduits dans la section Commentaires des entités auditées.

Nous tenons à souligner qu'elles ont adhéré à toutes les recommandations.

Recommandations au ministère du Travail, de l'Emploi et de la Solidarité sociale

1. **Réaliser une analyse d'impact pour recenser les systèmes d'information critiques et déterminer des objectifs de reprise informatique pour chacun d'eux.**
2. **Mettre en place des plans de reprise informatique pour les systèmes pour lesquels une telle stratégie a été retenue.**
3. **Fournir régulièrement à la haute direction de l'information adéquate concernant la reprise informatique afin qu'elle approuve les stratégies de reprise et en assure le suivi.**

Recommandation au ministère du Travail, de l'Emploi et de la Solidarité sociale et au Centre de services partagés du Québec

4. **S'assurer que les essais portant sur les plans de reprise informatique sont préparés adéquatement et réalisés comme il a été prévu.**

Recommandation au Centre de services partagés du Québec

5. **Informer ses clients sur les mesures de sauvegarde mises en place, notamment au sujet des environnements visés, du type de copies de sauvegarde et de leur fréquence, afin qu'ils puissent évaluer si ces mesures répondent à leurs besoins, ou convenir de mesures particulières, le cas échéant.**

Recommandations au Secrétariat du Conseil du trésor

6. **Préciser le contenu des documents d'encadrement concernant la reprise informatique dans le cadre de la gestion de la continuité des services.**
7. **Inclure dans la vision globale des ressources informationnelles qu'il doit développer l'enjeu de la reprise informatique.**
8. **Se doter des moyens lui permettant d'apprécier dans quelle mesure les plans de reprise informatique des ministères et organismes répondent aux besoins déterminés dans leur plan de continuité des services.**

Table des matières

Équipe

Marcel Couture
Vérificateur général adjoint

Carole Bédard
Directrice d'audit

Patrice Watier
Directeur d'audit

Annie Bernard
Daniel Blesa
Étienne Côté
Rachel Ladouceur

1 Mise en contexte

1 Les technologies de l'information jouent un rôle de plus en plus important dans la prestation de services aux citoyens et aux entreprises. Elles constituent des outils indispensables qui permettent au gouvernement de s'acquitter de ses responsabilités avec efficacité et efficience.

2 Comme le précise notre étude intitulée *Portrait de la gouvernance et de la gestion des technologies de l'information au gouvernement du Québec*, publiée dans notre tome de l'hiver 2017, la gestion de la continuité des services est considérée comme un des processus les plus vulnérables selon les hauts dirigeants et les responsables des technologies de l'information des ministères et organismes sondés.

3 Un plan de continuité des services vise à éviter ou à minimiser toute interruption des services essentiels en cas de sinistre. La reprise informatique est une constituante souvent indispensable de ce plan. En effet, des incidents, tels que la défaillance d'un équipement informatique, une panne électrique, une cyberattaque, la propagation d'un virus ou une catastrophe naturelle, pourraient causer la non-disponibilité des systèmes d'information et paralyser les services du gouvernement. Lorsqu'une organisation ne parvient pas à maintenir la disponibilité de ses systèmes d'information à la suite d'un incident majeur, elle peut mettre en œuvre des stratégies de reprise informatique pour rétablir ses services.

4 Selon le *Cadre de référence sur la continuité des services essentiels dans la fonction publique*, entré en vigueur en juin 2017, chaque ministère et organisme assujetti à la *Loi sur la fonction publique* doit se doter d'un plan de continuité des services essentiels et le tenir à jour. Ce plan comprend l'ensemble des procédures qui servent de guides aux organisations pour qu'elles puissent rétablir leurs services après un sinistre à un niveau de fonctionnement prédéfini. La figure 1 montre les principales étapes de l'élaboration du plan de continuité des services, lequel doit inclure, si nécessaire, les plans de reprise informatique.

Figure 1 Élaboration d'un plan de continuité des services

5 Une analyse d'impact consiste, pour une organisation, à évaluer les risques et les effets qu'aurait une interruption de ses services pour une période déterminée (pertes financières, incidences politiques, sécurité et santé des citoyens, etc.). Elle permet à la haute direction de recenser les services qu'elle considère comme essentiels à la réalisation de la mission, de déterminer les objectifs et les priorités relatifs à la continuité de ces services, ainsi que de déterminer la durée maximale d'interruption qu'elle peut tolérer.

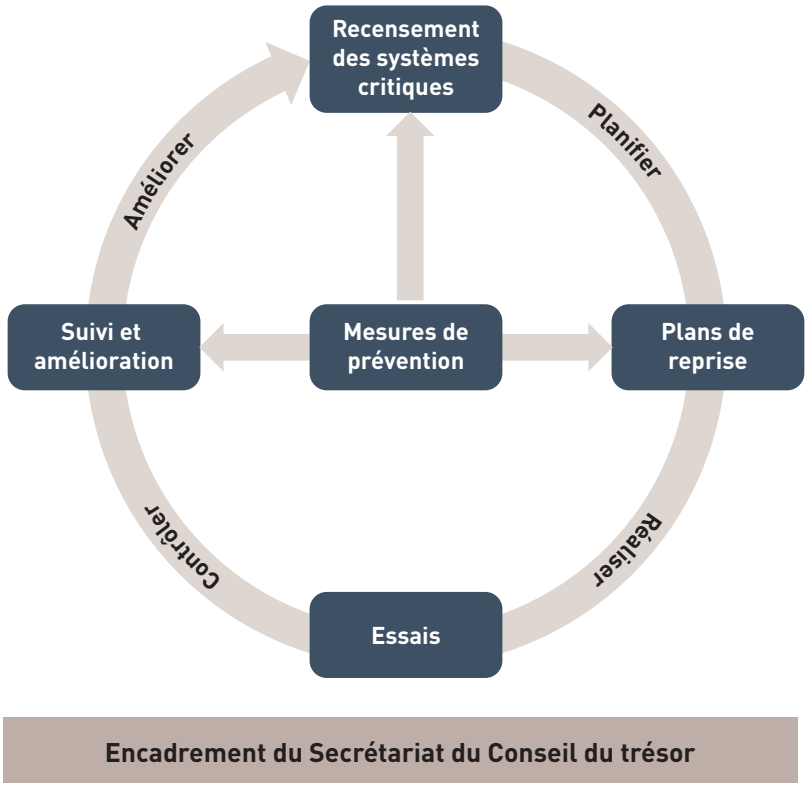
6 L'organisation doit également recenser les ressources indispensables à la prestation de ses services essentiels, dont les systèmes d'information critiques. Elle doit aussi évaluer différents scénarios relatifs à divers sinistres pouvant rendre ces ressources non disponibles.

7 Même si la probabilité qu'un sinistre survienne est difficile à évaluer parce qu'elle est souvent très faible, l'impact d'un tel sinistre sur l'organisation pourrait être important. Cette dernière doit donc élaborer des stratégies afin de réduire ce risque à un niveau acceptable. La haute direction doit analyser les avantages de mettre en place des stratégies en tenant compte des coûts et des délais liés à la reprise informatique par rapport aux autres possibilités (par exemple, le recours à des procédures manuelles), et ce, pour l'ensemble des systèmes d'information visés. Toutes les stratégies sont consignées dans un plan de continuité des services. Parties intégrantes du plan de continuité, les plans de reprise informatique comprennent les procédures à suivre et les ressources nécessaires pour la remise en service des systèmes critiques dans les délais attendus.

8 Enfin, la haute direction doit s'assurer du suivi et de la mise à jour de son plan de continuité, y compris des divers plans de reprise informatique, afin que ces plans évoluent au même rythme que l'organisation.

9 Dans le cadre de notre audit, nos travaux se sont concentrés principalement sur la gestion de la reprise informatique concernant les systèmes d'information critiques du ministère du Travail, de l'Emploi et de la Solidarité sociale (MTESS). La figure 2 en montre les principales étapes.

Figure 2 Cycle de gouvernance et de gestion de la reprise informatique



10 Parmi les nombreux services du MTESS qui reposent sur les technologies de l'information, mentionnons l'aide financière de dernier recours, le Régime québécois d'assurance parentale (RQAP), le registre de l'état civil et Services Québec. Ce dernier constitue un guichet multiservice qui permet un accès simplifié aux services publics.

11 Le MTESS est responsable de ses systèmes d'information. Cependant, il a confié la gestion de toutes les infrastructures technologiques liées à ses systèmes au Centre de services partagés du Québec (CSPQ), à l'exception de celles relatives au registre de l'état civil, qui sont gérées à l'interne.

Rôles et responsabilités

12 Les rôles et les responsabilités à l'égard des technologies de l'information et de la continuité des services sont déterminés, entre autres, par la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*, la *Directive sur la sécurité de l'information gouvernementale*, la *Loi sur la sécurité civile* et le *Plan national de sécurité civile*. Voici les entités que nous avons auditées et leurs principaux rôles et responsabilités en lien avec notre audit.

MTESS	■ Recenser les biens et les services essentiels offerts, s'enquérir des risques de sinistre majeur qui peuvent affecter ces biens et ces services, recenser les mesures de protection à l'égard de ces risques et établir, pour chaque bien ou service inventorié, la vulnérabilité de l'organisation eu égard aux risques ■ Établir et maintenir opérationnelles des mesures de protection destinées à réduire la vulnérabilité et, lorsque ces mesures sont essentielles au maintien ou au rétablissement de la fourniture des biens ou des services en situation de sinistre, désigner la personne chargée de les exécuter et ses substituts en précisant leur nom et leurs coordonnées ■ Assurer la gestion et la coordination du plan de continuité des services de l'organisation ■ S'assurer de la mise en œuvre des processus formels de sécurité de l'information, ce qui permet notamment d'assurer la gestion des risques de sécurité, dont le risque d'atteinte à la disponibilité ■ Effectuer une reddition de comptes périodique au Secrétariat du Conseil du trésor (SCT) à l'égard de la sécurité de l'information ■ Désigner un responsable de la continuité des services
CSPQ	■ Fournir ou rendre accessibles aux organismes publics les biens et les services dont ils ont besoin dans l'exercice de leurs fonctions, notamment en matière de ressources informationnelles ■ S'assurer de la mise en œuvre des processus formels de sécurité de l'information, ce qui permet notamment d'assurer la gestion des risques de sécurité, dont le risque d'atteinte à la disponibilité

SCT	■ Assurer la responsabilité de la mission Services essentiels gouvernementaux du *Plan national de sécurité civile* ■ Élaborer et proposer au gouvernement des politiques et des directives en matière de gouvernance et de gestion des ressources informationnelles, les mettre en œuvre et en coordonner l'exécution auprès des organismes publics ■ Effectuer un suivi du respect de la réglementation, analyser la reddition de comptes transmise par les ministères et organismes et formuler des recommandations en matière de gouvernance et de gestion des ressources informationnelles ■ Fournir aux organismes publics des outils, des guides, des pratiques, divers services et de l'assistance en matière de gouvernance et de gestion des ressources informationnelles, ce qui comprend la sécurité de l'information gouvernementale

13 Les objectifs de l'audit, les critères d'évaluation ainsi que la portée des travaux sont présentés en annexe.

2 Résultats de l'audit

14 Les travaux se sont articulés autour de deux axes, soit la gestion de la reprise informatique relative aux systèmes d'information critiques du MTESS et l'encadrement gouvernemental à cet égard.

2.1 Gestion de la reprise informatique

Recensement des systèmes d'information critiques

15 Comme le montre la figure 1, l'analyse d'impact doit permettre de déterminer notamment les services essentiels et les systèmes d'information indispensables à leur prestation. Elle vise également à déceler si des interdépendances entre les systèmes sont susceptibles de nuire à leur bon fonctionnement, et ce, afin d'assurer leur remise en service en cas de sinistre.

16 Le MTESS n'a pas réalisé d'analyse complète de l'impact et des risques liés à la non-disponibilité de ses systèmes d'information et à leurs interdépendances. Cette analyse lui aurait permis de recenser ses systèmes d'information critiques et de déterminer, pour ceux-ci, des objectifs et des priorités en matière de reprise.

17 Comme le MTESS n'a pas réalisé d'analyse complète de l'impact de la non-disponibilité des systèmes d'information critiques et de leurs interdépendances, il n'est pas en mesure de conclure, pour l'ensemble de ces systèmes, que les plans de reprise informatique permettraient le rétablissement de tous ses services essentiels en cas de sinistre. Une telle analyse permettrait de mettre en évidence des situations discutables. Par exemple, le RQAP, pour lequel un plan de reprise informatique a été produit, a comme porte d'entrée le service d'authentification gouvernementale clicSÉQUR – Citoyens qui, lui, ne fait pas l'objet d'un tel plan. Le MTESS pourrait mettre en place des mesures en cas de non-disponibilité de clicSÉQUR – Citoyens afin d'offrir les services liés au RQAP, et ce, par d'autres modes de prestation. Par contre, ces mesures ne sont pas consignées dans son plan de continuité des services.

18 Le MTESS a initialement élaboré son plan de continuité des services pour se préparer à une éventuelle pandémie d'influenza. Même si la haute direction du ministère a autorisé l'utilisation de ce plan pour faire face à tout type de sinistre et que celui-ci a été mis à jour régulièrement, il ne traite pas de l'impact de la non-disponibilité des systèmes d'information ni de la reprise informatique. De plus, il ne comporte aucun lien entre les services essentiels du MTESS et chacun des systèmes d'information indispensables à leur prestation. Il se concentre plutôt sur les mesures à mettre en place dans le cas où le ministère serait aux prises avec un fort taux d'absentéisme.

19 Le plan de continuité des services du MTESS inclut en annexe la liste actualisée des produits et des services informatiques jugés essentiels. Cette liste présente les systèmes à maintenir en service en cas de manque de personnel. Par contre, ces systèmes ne sont pas nécessairement ceux qui permettent de maintenir les services qui ont été qualifiés d'essentiels. Nous avons relevé des incohérences dans cette liste. Par exemple, un système d'information est jugé essentiel, alors qu'il est utilisé pour la prestation d'un service qui, lui, ne l'est pas.

Disponibilité et qualité des plans de reprise informatique

20 Les organismes doivent élaborer un plan de reprise informatique pour chacun des systèmes considérés comme critiques, et ce, afin de pouvoir les rétablir dans un délai acceptable en cas de sinistre. Ce plan doit notamment inclure toutes les ressources requises (personnes, installations physiques, infrastructures réseau, logiciels, etc.) et les procédures à suivre pour le mettre en œuvre.

21 Comme il a été mentionné précédemment, le MTESS a confié la gestion de l'ensemble des infrastructures (plateformes) relatives à ses systèmes d'information au CSPQ, à l'exception des infrastructures liées au registre de l'état civil, qui sont gérées à l'interne. Le MTESS a retenu les services du CSPQ selon deux principaux types d'offres de service. Pour la plateforme centrale, l'offre de service du CSPQ comprend la reprise informatique en cas de sinistre, alors que, pour la plateforme intermédiaire, la reprise informatique est offerte en option. Nous présentons ci-dessous les deux offres de service du CSPQ.

Offre de service	Importance	Reprise informatique en cas de sinistre
Plateforme centrale Plateforme applicative sur ordinateur central	La plateforme centrale joue un rôle clé au sein du gouvernement du Québec. Elle est utilisée par plus de 50 ministères et organismes. Elle permet notamment le traitement de la paie des fonctionnaires et de la rémunération des médecins. Pour le MTESS, elle permet la gestion de l'aide financière de dernier recours et le versement des prestations, notamment celles relatives à Emploi-Québec, au RQAP et à l'aide financière de dernier recours.	■ L'offre de service comprend la reprise informatique en cas de sinistre[1].

1. Afin d'offrir le service de reprise informatique, le CSPQ a conclu un contrat avec un fournisseur de services informatiques, ce qui lui permet d'utiliser un centre de traitement situé au Canada en cas de sinistre. Toutefois, pour le RQAP, la reprise informatique est prévue dans un autre centre de traitement géré par le CSPQ.

Offre de service	Importance	Reprise informatique en cas de sinistre
Plateforme intermédiaire Exploitation et maintien de solutions d'infrastructures	La plateforme intermédiaire est utilisée par 26 ministères et organismes. Elle inclut plus de 100 sites Web ainsi que 244 systèmes d'information qui permettent l'administration de programmes. Plusieurs de ces programmes sont essentiels pour le gouvernement et leur valeur en matière de budget s'élève à plusieurs milliards de dollars par année. Pour le MTESS, la plateforme intermédiaire permet notamment la gestion des services suivants : ■ le RQAP ; ■ tous les sites Web du ministère, dont Portail Québec, Urgence Québec et Emploi-Québec ; ■ le service d'authentification gouvernementale clicSÉQUR – Citoyens ; ■ les services en matière de relations de travail et d'information sur le travail.	■ L'offre de base n'inclut pas de plan de reprise informatique, mais elle prévoit la reprise dans les meilleurs délais. ■ L'option de reprise après sinistre offre un plan de reprise et le délai est adapté aux besoins des clients[1]. Cette option a été retenue pour six systèmes d'information gouvernementaux[2] seulement, dont un système du MTESS.

1. Afin d'offrir le service de reprise informatique, le CSPQ a conclu un contrat avec un fournisseur de services informatiques, ce qui lui permet d'utiliser un centre de traitement situé au Canada en cas de sinistre. Toutefois, pour le RQAP, la reprise informatique est prévue dans un autre centre de traitement géré par le CSPQ.
2. L'option de reprise après sinistre a été retenue pour les six systèmes d'information suivants : SAGIR (solutions d'affaires en gestion intégrée des ressources utilisées par plus de 70 ministères et organismes) ; UGO (solutions d'affaires en gestion intégrée des ressources utilisées par Revenu Québec) ; le RQAP (offert par le MTESS) ; le service de vente de permis de pêche et de chasse du ministère des Forêts, de la Faune et des Parcs ; le service de numérisation de la Commission des normes, de l'équité, de la santé et de la sécurité du travail ; le service de transfert sécurisé de fichiers du CSPQ.

22 Le MTESS n'a déterminé que partiellement les systèmes d'information qui appuient ses services essentiels. De plus, certains de ces systèmes ne font pas l'objet d'un plan de reprise. Toutefois, dans les cas où un plan de reprise a été produit, celui-ci est généralement complet.

23 Nos travaux visaient entre autres à nous assurer que chacun des systèmes d'information jugés critiques par le MTESS fait l'objet d'un plan de reprise informatique et que ce dernier est de qualité. Cependant, le ministère n'a pas établi de liste complète à cet égard. Par contre, il a effectué diverses démarches qui n'avaient pas pour objectif de recenser les systèmes devant faire l'objet d'un plan de reprise, mais qui ont tout de même permis d'en recenser quelques-uns. Nous avons donc utilisé un document produit par le ministère, soit la liste des actifs informationnels critiques et des mesures de contingence liées à ces actifs, ainsi que le plan de continuité des services.

24 Parmi les neuf systèmes d'information critiques que nous avons recensés, seulement trois font l'objet d'un plan de reprise informatique. Voici la description de ces neuf systèmes.

Système critique	Gestionnaire et offre de service	Disponibilité d'un plan de reprise	Description
Aide financière de dernier recours	CSPQ Plateforme centrale	Oui : reprise informatique dans un délai de 48 heures	■ Le système contient de l'information sur les bénéficiaires de l'aide sociale et il permet le versement mensuel des prestations qui leur sont dues. Ces prestations représentent souvent leur seule source de revenus. ■ En 2016-2017, 2,9 milliards de dollars ont été versés aux prestataires. Le nombre mensuel moyen de prestataires était de 335 167.
Régime québécois d'assurance parentale	CSPQ Plateforme intermédiaire	Oui : reprise informatique dans un délai de 24 heures	■ Le RQAP permet le versement de prestations aux travailleuses et aux travailleurs qui se prévalent d'un congé lors de la naissance ou de l'adoption d'un enfant. ■ En 2016-2017, 2,0 milliards de dollars ont été versés à 211 530 personnes. ■ Parmi les demandes de prestations effectuées, 90 % sont transmises en ligne.
Registre de l'état civil	MTESS Plateforme intermédiaire	Non[1]	■ Le système permet l'inscription d'information au registre de l'état civil du Québec et la délivrance de certificats pour différents événements de la vie : naissance, mariage, union civile, décès. ■ En 2016-2017, 171 000 inscriptions ont été enregistrées dans le registre et 357 000 certificats et copies d'acte ont été délivrés. ■ Parmi les demandes, 68 % sont transmises en ligne.
Service d'authentification clicSÉQUR – Citoyens	CSPQ Plateforme intermédiaire	Non	■ Ce service permet à une personne d'accéder de façon sécuritaire aux services en ligne des ministères et des organismes participants. ■ En 2017, ce service permettait l'accès à 23 services en ligne de 11 ministères et organismes, dont ceux de Revenu Québec, de Retraite Québec, de la Régie de l'assurance maladie du Québec, de l'Autorité des marchés financiers et du MTESS (RQAP, Directeur de l'état civil et Mon dossier citoyen). ■ Au 31 mars 2017, 1,7 million de citoyens étaient inscrits à ce service.
Site Web Urgence Québec	CSPQ Plateforme intermédiaire	Non	■ Le MTESS est responsable du volet communication du *Plan national de sécurité civile* et doit donc coordonner les communications des ministères et des organismes en situation d'urgence. Ce site Web constitue un outil d'information très important pour les citoyens.

1. Il faut toutefois noter qu'un environnement de relève dans un autre centre de traitement informatique avec réplication du système est disponible pour le registre de l'état civil.

Système critique	Gestionnaire et offre de service	Disponibilité d'un plan de reprise	Description
Système de courrier électronique	CSPQ Plateforme intermédiaire	Non	■ L'outil permet l'échange d'information et de documents. Il appuie certaines activités essentielles du MTESS, par exemple : — le soutien aux centres locaux d'emploi pour les programmes de solidarité sociale ; — les relations avec la clientèle.
Systèmes de gestion des services aux individus (trois systèmes importants)	CSPQ Plateforme centrale : un système	Oui pour le système hébergé sur la plateforme centrale : reprise informatique dans un délai de 48 heures	■ Les trois systèmes contiennent de l'information sur les participants aux programmes, aux mesures et aux services d'aide à l'emploi et d'accompagnement social, ainsi qu'à des programmes d'aide financière autres que ceux relatifs à l'aide financière de dernier recours. Ils permettent le versement mensuel des allocations.
	Plateforme intermédiaire : deux systèmes	Non pour les deux autres systèmes	■ En 2016-2017, 220 millions de dollars ont été versés (450 951 participations[2]).

2. Il s'agit du nombre de participations. Le nombre exact de personnes n'est pas disponible puisqu'une personne peut participer à plusieurs programmes ou mesures.

25 Lorsqu'un plan de reprise informatique est présent, nous nous sommes assurés de sa qualité. Le plan de reprise relatif à la plateforme centrale et celui portant sur le RQAP sont généralement complets puisqu'ils précisent bien toutes les ressources requises et les procédures à suivre pour leur mise en œuvre.

26 Par contre, la fonctionnalité permettant l'impression des chèques est exclue du plan de reprise relatif à la plateforme centrale pour le MTESS. En cas de sinistre, le ministère pourrait donc devoir procéder à l'émission de chèques manuels pour les prestataires qui ne reçoivent pas leurs versements par dépôt direct, soit environ 100 000 chèques par mois ou 18 % de tous les versements.

Essais périodiques

27 Des essais périodiques permettent à l'organisation de s'assurer que les procédures et la documentation traitant des ressources nécessaires au bon rétablissement des systèmes, prévues dans les plans de reprise informatique, sont adéquates. Ils servent aussi à s'assurer que toutes les étapes peuvent être réalisées dans les délais attendus. Rappelons que le délai est de 48 heures pour la plateforme centrale et de 24 heures pour le RQAP.

28 Pour la plateforme centrale, le CSPQ et les ministères et organismes clients ont convenu que deux essais portant sur le plan de reprise après sinistre seront réalisés annuellement. La même fréquence est prévue dans une entente pour le RQAP.

29 Depuis 2014-2015, la moitié des essais portant sur le plan de reprise relatif à la plateforme centrale a été annulée, dont tous ceux prévus en 2017-2018. Quant au RQAP, l'objectif de rétablir ce système dans un délai de 24 heures a été atteint cinq fois sur huit.

30 Selon le CSPQ et le MTESS, la non-disponibilité des professionnels pour réaliser les essais en dehors des heures normales de travail expliquerait l'annulation de certains essais portant sur le plan de reprise lié à la plateforme centrale depuis 2014-2015. Voici les résultats des essais liés aux plans de reprise de la plateforme centrale et du RQAP.

Année	Essais prévus (nbre)	Essais réalisés (nbre)	Résultats
Plateforme centrale (pour le MTESS)			
2014-2015	2	2	Lors des deux essais, des problèmes ont empêché la réalisation de certaines étapes.
2015-2016	2	1	Tous les objectifs importants ont été atteints.
2016-2017	2	1	Tous les objectifs importants ont été atteints.
2017-2018	2	0	Aucun essai n'a été réalisé.
RQAP			
2014-2015	2	2	Pour un des deux essais, l'objectif de la reprise informatique dans un délai de 24 heures n'a pas été atteint (2e essai : 44 heures).
2015-2016	2	2	Tous les objectifs importants ont été atteints.
2016-2017	2	2	Pour les deux essais réalisés, l'objectif de la reprise informatique dans un délai de 24 heures n'a pas été atteint (1er essai : 36 heures ; 2e essai : 23 jours).
2017-2018	2	2	L'essai d'octobre 2017 s'est avéré non concluant. Cependant, le MTESS et le CSPQ ont recommencé celui-ci en novembre et l'objectif de la reprise informatique dans un délai de 24 heures a été atteint. L'objectif a également été atteint pour l'essai de février 2018.

31 Le bilan de l'essai de l'hiver 2017 relatif au RQAP a fait état de plusieurs problèmes. En cas de sinistre réel, l'environnement technologique lié au RQAP aurait été rétabli en 23 jours. Le CSPQ a réalisé une analyse pour en déterminer les causes. Il s'avère que certaines procédures étaient incomplètes ou n'avaient pas été mises à jour adéquatement. Des mesures ont été prises à cet égard, ce qui a permis d'atteindre l'objectif de la reprise informatique dans un délai de 24 heures lors de l'essai de novembre 2017. Cela démontre l'importance de bien se préparer à la réalisation des essais afin de s'assurer du fonctionnement du plan de reprise et, le cas échéant, d'apporter les mesures correctrices appropriées.

Mesures de prévention des sinistres

32 Certaines mesures préventives permettent de diminuer les risques d'interruption des systèmes d'information ou favorisent une reprise informatique efficace. Elles sont présentées ci-dessous.

Mesure	Objectif	Bonnes pratiques
Gestion des copies de sauvegarde	■ Il s'agit d'un élément essentiel de tout plan de reprise informatique. En l'absence d'un plan, les copies de sauvegarde constituent le seul moyen de rétablir un système et ses données.	■ Les mesures de sauvegarde concernant les systèmes et les données doivent être consignées dans un document. Elles doivent décrire notamment : — la fréquence des copies ; — la durée et le lieu de conservation hors site. ■ Des tests sur les procédures de récupération des systèmes et de leurs données doivent être réalisés régulièrement afin d'en assurer la disponibilité et l'intégrité.
Gestion des incidents	■ La gestion des incidents permet à l'organisation de détecter les incidents et d'y réagir rapidement afin de minimiser la durée de la non-disponibilité des systèmes. Une mauvaise réaction peut transformer un incident mineur en un incident majeur.	■ Chaque incident doit être enregistré, analysé et priorisé afin que l'organisation puisse améliorer sa compréhension de celui-ci et apporter les mesures correctrices appropriées.
Sécurité physique des centres de traitement informatique	■ La sécurité physique vise à diminuer le risque que les centres de traitement informatique soient endommagés.	■ Des contrôles doivent être mis en place, par exemple : — des contrôles pour limiter l'accès au personnel autorisé seulement ; — des systèmes de détection et de prévention des incendies, des inondations et des interruptions électriques ; — des contrôles de la température ambiante.

33 L'offre de service du CSPQ concernant les mesures de sauvegarde manque de précision. De plus, la documentation relative aux mesures de sauvegarde ne porte pas sur l'ensemble des systèmes du MTESS pour lesquels le CSPQ offre des services.

34 Le MTESS et le CSPQ effectuent des copies de sauvegarde des données et des systèmes et les conservent dans un site externe. L'offre de service du CSPQ comprend la réalisation de copies de sauvegarde pour une durée de conservation de 45 jours. Par contre, le CSPQ ne précise pas plusieurs autres éléments, tels que la fréquence des copies, le type de sauvegarde (complète ou partielle) et les environnements visés. Le MTESS et le CSPQ avaient déjà convenu des mesures de sauvegarde à mettre en place en 2014, mais la documentation relative à celles-ci n'est plus à jour. Le ministère ne peut pas donc s'assurer que les copies de sauvegarde effectuées par le CSPQ permettent de garantir l'intégrité et la disponibilité des données de l'ensemble de ses systèmes. Cela est particulièrement important pour les systèmes ne faisant pas l'objet d'un plan de reprise, puisque les copies de sauvegarde constituent le seul moyen de les remettre en service dans les meilleurs délais. Dans les faits, nous avons relevé deux systèmes mis en place depuis 2014 pour lesquels le MTESS a signifié ses besoins au CSPQ, et ces derniers ont consigné les mesures de sauvegarde relatives à ces systèmes dans un document.

35 Par ailleurs, la gestion des incidents effectuée par le MTESS et le CSPQ est adéquate. Les mesures liées à la sécurité physique des centres de traitement informatique du MTESS (registre de l'état civil) et du CSPQ le sont également. Les contrôles d'accès pour le personnel autorisé sont bien en place et les systèmes de sécurité nécessaires sont présents.

Suivi des résultats et amélioration continue

36 Pour favoriser la continuité des services et la reprise informatique et pour bien répondre aux besoins de l'organisation, la haute direction doit veiller régulièrement à ce que les politiques, les stratégies et les plans de reprise soient actualisés. Elle doit également être informée adéquatement de tous les risques importants et des enjeux à cet égard.

37 La haute direction du MTESS n'effectue pas de suivi des plans de reprise informatique liés à ses systèmes, qui appuient son plan de continuité des services. De plus, les décisions quant au choix des stratégies de reprise informatique et les objectifs liés aux délais de reprise n'ont pas fait l'objet de discussions au comité exécutif du ministère.

38 Les seules mentions relatives au plan de continuité des services qui sont incluses dans les procès-verbaux du comité exécutif du MTESS portent sur son autorisation et sa mise à jour. La reprise informatique n'y est pas abordée. Pourtant, il serait important que la haute direction revoie régulièrement les objectifs liés aux délais de reprise informatique, qu'elle approuve les stratégies de reprise et qu'elle soit informée des résultats des essais liés aux plans de reprise informatique.

39 D'autre part, le MTESS et le CSPQ devraient se concerter afin de mettre à jour la documentation à l'égard de certains éléments, dont les suivants :

- les mesures de sauvegarde ;
- les stratégies de reprise informatique (liste des systèmes, délais de reprise, rôles et responsabilités, modalités de réalisation des essais, etc.) ;
- la reddition de comptes s'y rapportant.

Recommandations

40 Les recommandations suivantes s'adressent au ministère du Travail, de l'Emploi et de la Solidarité sociale.

1 **Réaliser une analyse d'impact pour recenser les systèmes d'information critiques et déterminer des objectifs de reprise informatique pour chacun d'eux.**

2 **Mettre en place des plans de reprise informatique pour les systèmes pour lesquels une telle stratégie a été retenue.**

3 **Fournir régulièrement à la haute direction de l'information adéquate concernant la reprise informatique afin qu'elle approuve les stratégies de reprise et en assure le suivi.**

41 La recommandation suivante s'adresse au ministère du Travail, de l'Emploi et de la Solidarité sociale et au Centre de services partagés du Québec.

4 **S'assurer que les essais portant sur les plans de reprise informatique sont préparés adéquatement et réalisés comme il a été prévu.**

42 La recommandation suivante s'adresse au Centre de services partagés du Québec.

5 **Informer ses clients sur les mesures de sauvegarde mises en place, notamment au sujet des environnements visés, du type de copies de sauvegarde et de leur fréquence, afin qu'ils puissent évaluer si ces mesures répondent à leurs besoins, ou convenir de mesures particulières, le cas échéant.**

2.2 Encadrement gouvernemental

43 Depuis mars 2016, le SCT est responsable de la mission Services essentiels gouvernementaux incluse dans le *Plan national de sécurité civile*. Celle-ci consiste notamment à assurer la continuité des services essentiels de l'ensemble du gouvernement en cas de sinistre. À cet égard, le SCT a publié le *Cadre de référence sur la continuité des services essentiels dans la fonction publique* de même que le *Guide pratique pour la conception d'un plan de continuité des services essentiels*.

44 Ainsi, les hauts dirigeants des ministères et organismes doivent s'assurer de la disponibilité de leurs **services essentiels**, soit de ceux qui répondent à la définition gouvernementale formulée dans ces documents. Toutefois, si leur organisation fournit des services qui ne répondent pas à cette définition, ces hauts dirigeants doivent déterminer, parmi ceux-ci, les services jugés essentiels à la réalisation de la mission et mettre en place les mesures nécessaires permettant d'assurer la disponibilité de ces services. À cet égard, la *Directive sur la sécurité de l'information gouvernementale* indique que les organismes publics sont responsables d'assurer la disponibilité de l'information gouvernementale qu'ils détiennent dans l'exercice de leurs fonctions.

Les services essentiels sont ceux dont la perturbation pourrait mettre en péril la vie, la sécurité, la santé ou le bien-être économique de la personne dans une partie ou dans la totalité de la population.

45 Au sein du SCT, le dirigeant principal de l'information est responsable d'assurer l'application de cette directive et d'accompagner les ministères et organismes à cet égard en mettant à leur disposition des pratiques exemplaires. En ce qui concerne les **risques de sécurité de l'information à portée gouvernementale**, le dirigeant principal de l'information a la responsabilité de veiller à ce que ceux-ci soient recensés et adéquatement pris en charge. Dans ce cadre, il constitue et maintient un registre des risques à portée gouvernementale qu'il recense annuellement auprès des ministères et organismes. Son intervention vise notamment à recueillir de l'information sur les stratégies de traitement des risques et à disposer d'une cartographie à jour des interdépendances en matière de risques à portée gouvernementale. Elle vise également à connaître le niveau d'acceptabilité des risques résiduels des entités gouvernementales et à prendre les mesures requises afin qu'elles réduisent leurs risques à un niveau acceptable.

Les risques de sécurité de l'information à portée gouvernementale sont ceux qui sont susceptibles de porter atteinte à la sécurité de l'information gouvernementale et qui peuvent avoir des conséquences graves sur :

- la prestation des services indispensables à la population ;
- la prestation de services d'autres organismes publics ;
- la vie, la santé ou le bien-être des personnes ;
- le respect des droits fondamentaux à la protection des renseignements personnels et le respect de la vie privée ;
- l'image du gouvernement.

46 En décembre 2017, divers changements ont été apportés à la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*, lesquels visent à la renforcer. Par exemple, le dirigeant principal de l'information doit maintenant développer et soumettre au Conseil du trésor une vision globale en matière de ressources informationnelles. Il doit également favoriser l'adéquation entre, d'une part, les priorités gouvernementales et les priorités des organismes publics et, d'autre part, les possibilités qu'offrent les ressources informationnelles pour soutenir les projets de transformation et les activités courantes de ces organismes. De plus, sur recommandation du Conseil du trésor, le gouvernement peut exiger qu'un organisme public utilise les services en ressources informationnelles du CSPQ. La plupart des nouvelles dispositions sont entrées en vigueur le 7 mars 2018.

47 Les documents d'encadrement du SCT ne sont pas assez précis quant à l'importance et au rôle des plans de reprise informatique à l'intérieur d'un processus global de gestion de la continuité des services. Bien que le SCT ait recensé de l'information auprès des ministères et organismes sur leurs plans de reprise informatique, celle-ci ne lui permet pas d'apprécier l'adéquation de ces plans avec leur plan de continuité des services.

48 Les plans de reprise informatique ne peuvent être élaborés de façon isolée. Ils doivent tenir compte de l'analyse d'impact et faire partie d'un processus global de gestion de la continuité des services. Deux guides publiés par le SCT abordent le sujet de la continuité des services. Selon le *Guide de catégorisation de l'information*, la démarche proposée dans ce document peut notamment servir d'intrant pour la mise en œuvre des stratégies de continuité. L'approche est différente de celle utilisée dans le *Guide pratique pour la conception d'un plan de continuité des services essentiels*, laquelle est fondée sur la prestation des services. Les orientations du SCT ne précisent pas que les plans de reprise informatique doivent être intégrés dans le plan de continuité des services et elles donnent peu d'information sur la démarche d'élaboration des plans de reprise. De telles précisions permettraient de favoriser une plus grande uniformité au sein du gouvernement.

49 Certaines exigences énoncées par le gouvernement du Canada en matière de reprise informatique sont plus précises. Par exemple, les cadres supérieurs doivent entre autres garantir que la continuité des services s'appuie sur des plans de continuité des technologies de l'information, c'est-à-dire sur des plans de reprise informatique. De plus, le coordonnateur de la sécurité des technologies de l'information et le coordonnateur de la planification de la continuité des activités doivent collaborer pour utiliser une approche globale de la prestation continue des services.

50 Au Québec, le dirigeant principal de l'information doit déposer tous les deux ans au Conseil du trésor un rapport sur l'état de situation gouvernementale de la sécurité de l'information. En 2016, il a demandé aux ministères et organismes s'ils avaient mis en place des processus leur permettant de s'assurer de la disponibilité de l'information, notamment des plans de reprise informatique. Ainsi, le SCT collecte de l'information sur l'existence de ces plans, mais il nous a confirmé qu'il tient pour acquis que ceux-ci sont opérationnels et périodiquement testés.

51 Comme nous l'avons mentionné précédemment, le CSPQ offre en option aux ministères et organismes qui utilisent la plateforme intermédiaire un service de reprise après sinistre. L'offre de base du CSPQ, qui n'inclut pas ce service, prévoit que les systèmes hébergés sur cette plateforme seront rétablis dans les meilleurs délais, mais ces délais ne sont pas précisés. Il est donc difficile pour les entités utilisant cette plateforme d'évaluer les conséquences possibles d'un sinistre. Il faut toutefois préciser que la plateforme intermédiaire du CSPQ n'est actuellement utilisée que par 26 ministères et organismes. D'autres entités ont leurs propres infrastructures et certains de leurs systèmes font l'objet d'un plan de reprise informatique. La situation pourrait cependant changer de manière significative si le gouvernement décidait d'exiger des organismes publics qu'ils utilisent davantage les services en ressources informationnelles du CSPQ, comme le lui permettent les nouvelles dispositions de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*.

Recommandations

52 Les recommandations suivantes s'adressent au Secrétariat du Conseil du trésor.

6 **Préciser le contenu des documents d'encadrement concernant la reprise informatique dans le cadre de la gestion de la continuité des services.**

7 **Inclure dans la vision globale des ressources informationnelles qu'il doit développer l'enjeu de la reprise informatique.**

8 **Se doter des moyens lui permettant d'apprécier dans quelle mesure les plans de reprise informatique des ministères et organismes répondent aux besoins déterminés dans leur plan de continuité des services.**

Commentaires des entités auditées

Les entités auditées ont eu l'occasion de transmettre leurs commentaires, qui sont reproduits dans la présente section. Nous tenons à souligner qu'elles ont adhéré à toutes les recommandations.

Commentaires du Centre de services partagés du Québec

« Le Centre adhère aux recommandations du Vérificateur général. À cet égard, il entend poursuivre ses travaux afin de s'assurer que les processus et la documentation nécessaires à la réalisation des essais font l'objet d'un suivi constant afin d'assurer le succès des essais de reprise réalisés.

« Le Centre informera ses clients sur les particularités associées aux mesures de sauvegarde en place afin qu'ils comprennent bien la portée des services rendus et les impacts à l'égard de la reprise informatique pour leur organisation. Cependant, le Centre ne pourra pas se substituer aux ministères et organismes pour les plans de continuité et le choix du plan de reprise. »

Commentaires du ministère du Travail, de l'Emploi et de la Solidarité sociale

« Le ministère souscrit aux recommandations du Vérificateur général. De ce fait, il s'engage à donner suite à celles-ci en poursuivant les travaux en cours ou en entreprenant les travaux complémentaires requis.

« Le ministère tient à rappeler que, pour le versement des prestations d'aide financière de dernier recours et de l'assurance parentale, soit sa mission principale, la reprise informatique est présente. Cette situation permettrait donc au ministère, en cas de sinistre, de maintenir les versements.

« Par ailleurs, plusieurs travaux en lien avec les recommandations sont déjà en cours, notamment la révision du plan de continuité des activités essentielles et la catégorisation des actifs critiques. D'ailleurs, pour le plan de continuité des activités essentielles incluant la reprise des systèmes d'information indispensables à leur prestation, les travaux sont réalisés en conformité avec les attentes du Secrétariat du Conseil du trésor exprimées dans le *Cadre de référence sur la continuité des services essentiels dans la fonction publique*.

« Parmi les autres travaux en cours, on retrouve la mise en place de la reprise informatique pour le site Web Urgence Québec et pour le registre de l'état civil.

« Le ministère prend au sérieux les essais de reprise. En effet, comme mentionné dans le rapport, après avoir rencontré des difficultés pour un essai de reprise pour le RQAP, des mesures ont été prises pour permettre de régler la situation. D'ailleurs, les objectifs ont été atteints pour les essais subséquents.

« Finalement, le ministère tient à souligner que plusieurs travaux réalisés au cours des dernières années ont permis d'améliorer la situation au regard de la continuité de ses services, notamment ceux liés à la mise à niveau technologique inscrits dans la stratégie visant à contrer la désuétude et à assurer l'évolution des services. »

Commentaires du Secrétariat du Conseil du trésor

« Le Secrétariat du Conseil du trésor accueille favorablement les recommandations formulées par le Vérificateur général. Le Secrétariat est soucieux de maintenir une approche stratégique qui permet aux ministères et aux organismes de relever les enjeux actuels et futurs en matière de sécurité de l'information. D'ailleurs, dès 2014, une nouvelle directive sur la sécurité de l'information ainsi que des cadres de gestion afférents étaient mis en place.

« Le Secrétariat entend donc poursuivre la démarche entreprise et s'assurer de l'amélioration continue de l'encadrement des pratiques, des outils, des guides et de l'assistance en sécurité de l'information. Les recommandations du Vérificateur général portant sur la reprise informatique concourent favorablement à cette démarche. »

Annexe et sigles

Annexe Objectifs de l'audit et portée des travaux

Sigles

CSPQ	Centre de services partagés du Québec	**RQAP**	Régime québécois d'assurance parentale
MTESS	Ministère du Travail, de l'Emploi et de la Solidarité sociale	**SCT**	Secrétariat du Conseil du trésor

Annexe Objectifs de l'audit et portée des travaux

Objectifs de l'audit

Le présent rapport de mission d'audit indépendant fait partie du tome de mai 2018 du *Rapport du Vérificateur général du Québec à l'Assemblée nationale pour l'année 2018-2019*.

La responsabilité du Vérificateur général consiste à fournir une conclusion sur les objectifs propres à la présente mission d'audit. Pour ce faire, nous avons recueilli les éléments probants suffisants et appropriés pour fonder nos conclusions et pour obtenir un niveau d'assurance raisonnable.

Notre évaluation est basée sur les critères que nous avons jugés valables dans les circonstances et qui sont exposés ci-après.

Ces critères sont basés sur les bonnes pratiques reconnues en matière de reprise informatique (ISO/CEI 27002, ISO/CEI 27031, ISO 22301, COBIT 5).

Objectifs de l'audit	Critères d'évaluation
Déterminer si le MTESS et le CSPQ prennent les mesures nécessaires pour répondre aux risques d'interruption de service pouvant affecter la disponibilité des systèmes d'information que le MTESS juge critiques (soit ceux pour lesquels une reprise informatique est nécessaire rapidement).	■ Un système de gestion de la continuité des services a été élaboré et mis en œuvre, lequel comprend notamment : — une politique de continuité approuvée par la haute direction ; — le recensement des processus organisationnels critiques ; — l'analyse des impacts d'une interruption de service et la détermination des priorités, des objectifs et des cibles de continuité en matière d'activités et de reprise ; — le partage des rôles et responsabilités. ■ Les systèmes d'information critiques sont déterminés et les stratégies de reprise informatique retenues répondent aux besoins organisationnels. ■ Les plans de reprise informatique pour les systèmes jugés critiques par le ministère sont disponibles et comprennent notamment la documentation des ressources requises (personnes, installations physiques, infrastructures réseau, logiciels, etc.) et les procédures à suivre pour la reprise. ■ Les plans de reprise font l'objet d'essais périodiques et d'une amélioration continue. ■ Des mesures de prévention des sinistres, telles que la gestion des incidents majeurs, la gestion des copies de sauvegarde et la sécurité physique des centres de traitement informatique, sont mises en œuvre. ■ La direction s'assure périodiquement que les objectifs de continuité sont atteints et que les priorités de reprise demeurent appropriées. Des mesures correctrices sont mises en œuvre si nécessaire.
S'assurer que le SCT apporte un encadrement et un soutien appropriés en matière de reprise informatique aux ministères et organismes assujettis à la *Loi sur l'administration publique*.	■ Des politiques et des directives sont élaborées, mises en œuvre et suivies auprès des ministères et organismes publics. ■ Des outils, des guides et du soutien sont offerts aux ministères et organismes publics.

Les travaux d'audit dont traite ce rapport ont été menés en vertu de la *Loi sur le vérificateur général* et conformément aux méthodes de travail en vigueur. Ces méthodes respectent les Normes canadiennes de missions de certification (NCMC) présentées dans le *Manuel de CPA Canada – Certification*, notamment la norme sur les missions d'appréciation directe (NCMC 3001).

De plus, le Vérificateur général applique la Norme canadienne de contrôle qualité 1. Ainsi, il maintient un système de contrôle qualité qui comprend des politiques et des procédures documentées 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, le Vérificateur général s'est conformé aux règles sur l'indépendance et aux autres règles de déontologie prévues dans son code de déontologie.

Portée des travaux

Le présent rapport a été achevé le 12 avril 2018.

Nos travaux ont porté sur la gestion de la reprise informatique pour les systèmes d'information critiques du MTESS et sur l'encadrement fait par le SCT à cet égard. Ils n'avaient pas pour but de remettre en cause le recensement des services essentiels effectué par le MTESS.

Le MTESS a confié la gestion de l'ensemble des infrastructures (plateformes) relatives à ses systèmes d'information au CSPQ, à l'exception des infrastructures liées au registre de l'état civil, qui sont gérées à l'interne.

Nous avons effectué des entrevues et des échanges auprès de gestionnaires et de professionnels du MTESS, du CSPQ et du SCT. De plus, nous avons analysé divers documents provenant, entre autres, des systèmes d'information des entités auditées. Nous avons également fait des visites d'observation dans deux centres de traitement informatique. Nous n'avons pas procédé à un échantillonnage statistique, mais nous avons obtenu des données provenant des systèmes d'information relatifs à la gestion des incidents. Des comparaisons avec d'autres administrations publiques ont aussi été effectuées.

Nos travaux se sont déroulés principalement de mars à décembre 2017. Ils ont porté sur les exercices 2014-2015 à 2016-2017. Toutefois, certaines analyses peuvent avoir trait à des situations antérieures ou postérieures à cette période.

Les recommandations formulées à la suite de ces travaux s'adressent aux entités auditées. Les résultats de notre audit ne peuvent être extrapolés à l'ensemble des organismes publics, mais ils donnent des indications sur les bonnes pratiques et les éléments que les acteurs doivent prendre en compte.