Bureau du vérificateur général de l'Ontario

Audit de l'optimisation des ressources :

Sécurité et exploitation des systèmes de TI

Décembre 2023

Sécurité et exploitation des systèmes de TI

1.0 Résumé

Le gouvernement de l'Ontario possède un vaste portefeuille de plus de 1 200 systèmes de technologie de l'information (TI) qui assurent le fonctionnement des programmes provinciaux dans l'ensemble de la fonction publique de l'Ontario (FPO). Ces systèmes de TI revêtent une importance croissante pour la population et les entreprises de l'Ontario, car ils interviennent dans la prestation des services gouvernementaux en des domaines tels que l'éducation, le bien-être de l'enfance, l'aide sociale et l'information financière.

Pour gérer judicieusement ces systèmes, le gouvernement a structuré les activités de TI à ses 29 ministères en 8 groupes appelés groupements de TI. Les groupements apportent quotidiennement un soutien aux activités des ministères qui s'y rapportent, notamment en ce qui touche la mise en oeuvre des systèmes de TI, le soutien technique, la protection des données confidentielles, l'accès accordé au personnel compte tenu de son rôle en milieu de travail, l'examen des incidents critiques de TI (journaux d'audit), le suivi de l'évolution de la vigueur des systèmes de TI et la gestion des fournisseurs de TI et de leur rendement. Les huit groupements de TI sont chacun sous la gouverne d'un dirigeant principal de l'information (DPI), chargé d'appuyer les besoins en TI des ministères compris dans chaque groupement. De plus, les groupements de TI relèvent indirectement (sur le plan administratif) du Bureau du directeur général de l'information pour la fonction publique (DGIFP), responsable des besoins en TI à l'échelle du gouvernement provincial.

L'audit exposé ici porte sur quatre des huit groupements de TI afin d'évaluer la sécurité et la performance des systèmes et processus de TI employés dans l'exécution des programmes et services gouvernementaux. Nous avons sélectionné un échantillon de systèmes de TI dans les quatre grappes.

L'audit a permis de passer en revue et de scruter les mesures de contrôle de sécurité comme la politique sur les mots de passe et les paramètres des mots de passe afin d'analyser l'adhésion et la conformité aux normes sectorielles et à la politique sur les mots de passe au sein de la FPO. De plus, l'audit a permis d'évaluer s'il y avait dans les groupements de TI un processus en vue d'activer en temps voulu des rustines de sécurité d'une importance cruciale aux bases de données et systèmes de TI afin d'atténuer le risque de failles à la cybersécurité. Nous avons également passé en revue l'accès au système pour déterminer si les mesures de contrôle étaient, en ce qui touche leur conception et leur fonctionnement, performantes dans la distinction des tâches, la suppression en temps voulu de l'accès des employés licenciés et l'examen périodique de l'accès des superutilisateurs afin que l'accès aux comptes privilégiés fasse l'objet d'une distinction adéquate et soit réservé au personnel autorisé.

En outre, nous avons passé en revue les mesures de contrôle en place quant à la tenue des journaux d'audit des renseignements très confidentiels, notamment pour déterminer si on avait suivi adéquatement l'évolution des journaux d'audit, si on avait saisi dans les journaux d'audit les incidents critiques nécessaires à la surveillance des activités exécutées par le personnel et si les modalités de conservation étaient en phase avec les règlements de la FPO.

Nous avons aussi passé en revue divers indicateurs de rendement clés des activités qui témoignent du rendement des systèmes de TI pour faire en sorte qu'ils soient jaugés et qu'on en rende compte avec cohérence. En outre, nous avons passé en revue les mesures de contrôle permettant de suivre l'évolution du rendement des fournisseurs de TI ainsi que les documents permettant d'analyser si les groupements de TI faisaient rapport du rendement des fournisseurs et tiraient parti des contrats en vigueur avec les fournisseurs de TI afin d'éviter le dédoublement et la redondance dans les services.

Publication restreinte

Dans l'ensemble, nous avons constaté que la FPO continue de mettre en oeuvre un certain nombre de contrôles pour améliorer sa sécurité. Toutefois, notre audit a permis de cerner des aspects à améliorer et des contrôles qui doivent être davantage renforcés. Compte tenu de la nature délicate de nos constatations dans l'audit et des systèmes de TI connexes, les détails s'y rapportant n'ont pas été publiés dans le *Rapport annuel 2023* afin de limiter les risques encourus par la FPO. Cependant, les détails pertinents de nos constatations et recommandations sont parvenus au DGIFP et aux groupements de TI respectifs en vue de corriger la situation. Le DGIFP et les groupements ont souscrit aux recommandations et nous avons obtenu leur engagement à agir en temps voulu afin de mettre en oeuvre intégralement nos recommandations.

Puisque nos constatations sont de nature systémique, nous croyons que tous les groupements de TI de la FPO doivent les prendre en considération. C'est donc dire que nous recommandons aussi au DGIFP et aux groupements que nous n'avons pas passés en revue au cours de notre audit de voir ensemble si nos recommandations s'appliquent à eux et, le cas échéant, de mettre en oeuvre celles qui sont de mise.

RÉPONSE GLOBALE

Nous apprécions le travail accompli par le Bureau du vérificateur général de l'Ontario dans la préparation du présent rapport. La FPO s'est engagée à protéger les données confiées au gouvernement par la population et les entreprises de l'Ontario et elle s'efforce toujours d'améliorer ses pratiques de cybersécurité.

La FPO continue de travailler en vue d'améliorer ses contrôles et pratiques de sécurité actuels afin de faire face à l'évolution rapide des menaces à la sécurité mondiale et de permettre la réalisation d'engagements à l'égard de la prestation de services numériques sécurisés pour la population de l'Ontario. Le Bureau du directeur général de l'information pour la fonction publique et les groupements de TI souscrivent aux recommandations du BVGO et ils s'engagent à les respecter et à collaborer avec tous les groupements de TI et les divisions internes pour les mettre en oeuvre intégralement en temps opportun.

2.0 Contexte

2.1 Aperçu

Le gouvernement provincial se sert de plus de 1 200 systèmes de technologie de l'information (TI) dans l'exécution de ses programmes et la prestation de services à la population de l'Ontario. La gestion de ces systèmes chez les 29 ministères du gouvernement a été structurée en 8 groupes appelés groupements de TI. Ces groupements sont responsables des activités quotidiennes des TI dans les ministères qu'ils soutiennent, de la mise en oeuvre des nouveaux systèmes de TI et du suivi de la gestion des activités des TI ayant trait aux systèmes en cours en vue de la prestation des programmes et

services gouvernementaux. Les groupements doivent également rendre compte de la sécurité et de l'intégrité des données traitées et stockées dans leurs systèmes et bases de données.

Les huit groupements de TI sont chacun sous la gouverne d'un dirigeant principal de l'information (DPI), qui rend des comptes au sous-ministre de l'un des ministères compris dans le groupement. De plus, ces groupements relèvent indirectement du Bureau du directeur général de l'information pour la fonction publique (DGIFP), responsable des besoins en TI à l'échelle du gouvernement provincial. Le DGIFP, par le truchement de ses divisions intégrées, donne des conseils aux groupements : pour ce faire, il met en place des politiques et des modalités en ce qui touche des domaines tels que la cybersécurité, les politiques sur les mots de passe, le suivi de la vigueur des systèmes de TI et la mesure du rendement des fournisseurs de TI. Les groupements sont chargés de veiller à ce que la sécurité des données et les processus des activités soient en phase et en conformité avec les exigences énoncées dans les politiques et normes établies par le DGIFP. Notre Bureau a audité le DGIFP et ses trois divisions intégrées dans le cadre de notre audit de l'optimisation des ressources du Bureau du dirigeant principal de l'information pour la fonction publique de 2022.

2.2 Rôle des groupements de TI

Les groupements sont chargés de fournir aux ministères des services technologiques à l'appui de certains programmes gouvernementaux destinés aux Ontariens. Leurs responsabilités particulières sont les suivantes :

- rendre obligatoire les mots de passe sécuritaires pour protéger les systèmes de TI;
- passer en revue à intervalles réguliers les attestations dans la gestion de l'accès aux systèmes de TI;
- veiller à l'à-propos de l'accès privilégié des superutilisateurs aux systèmes de TI;
- tenir des journaux d'audit des incidents critiques et les passer en revue en temps voulu;
- jauger la vigueur des systèmes de TI à l'aide de paramètres et d'objectifs de service établis;
- gérer les fournisseurs de services de TI et faire le suivi de leur rendement;
- concevoir des modalités uniformes des activités pour en favoriser l'exécution cohérente par le personnel qui dispose d'un savoir et d'outils à cet égard.

Les groupements comptent sur le DGIFP pour obtenir des conseils sur la gestion et l'exécution de ces activités suivant les politiques et normes de TI qu'il détermine.

2.3 Sécurité et intégrité des systèmes de TI

L'absence de systèmes de TI bien conçus ou de mesures de contrôle vigoureuses présente plusieurs risques : l'accès aux données confidentielles et leur divulgation sans autorisation; l'atteinte à la protection des données; la prestation de services insatisfaisants par les fournisseurs. Les groupements de TI interviennent à cet égard par l'instauration de mesures de contrôle permettant de déceler et de prévenir les risques de collusion et de fraude et d'analyser la performance dans la gestion des systèmes de TI. Parmi ces mesures de contrôle, il y a les mots de passe sécuritaires, l'accès restreint et contrôlé aux systèmes de TI et le suivi périodique des journaux d'audit. Voici une courte description des mesures névralgiques de contrôle de la TI.

2.3.1 Sécurité des données (mesures de contrôle par mot de passe)

Les mots de passe servent de premier mécanisme de protection contre les menaces à la cybersécurité et permettent aux équipes des TI d'assurer la sécurité et la fiabilité des données confidentielles. Il importe que les organisations observent la politique qu'elles ont établie en la matière. Cette politique doit au moins définir les exigences relatives aux mots de passe des systèmes de TI. Voici quelques caractéristiques répandues dans les politiques sur les mots de passe sécuritaires :

- **Complexité des mots de passe** : Souvent, dans les politiques relatives aux mots de passe, on exige que ceux-ci répondent à certains critères de complexité, ce qui peut se traduire par l'intégration des éléments suivants :
  - Un nombre minimal de caractères requis (huit caractères).
  - Un agencement de lettres majuscules (A-Z) et minuscules (a-z), de chiffres (0-9) et de caractères spéciaux (!@#$&).
- **Expiration des mots de passe** : Il est possible que les mots de passe viennent à expiration à la suite d'une période définie, après quoi les utilisateurs devront les changer. De cette façon, dans l'éventualité d'une atteinte à la sécurité, on évite de s'y exposer longtemps.
- **Réutilisation des mots de passe** : Les politiques relatives aux mots de passe renferment souvent une règle qui interdisent de réutiliser un certain nombre de fois les mots de passe précédents.

Les mots de passe insécuritaires peuvent présenter un risque important à cet égard. Par exemple, lorsqu'il y a réutilisation des mots de passe, à savoir l'utilisation à plusieurs reprises des mêmes mots de passe ou de mots de passe semblables dans plusieurs comptes, l'accès sans autorisation des pirates informatiques s'en trouve facilité. Instaurer des politiques relatives à l'historique des mots de passe constitue une mesure de sécurité fondamentale qui permet de protéger les comptes et les données confidentielles des utilisateurs contre les accès sans autorisation et les atteintes à la vie privée.

2.3.2 Authentification multifactorielle

L'authentification multifactorielle consiste en un processus d'ouverture de session en plusieurs étapes auquel s'ajoute un mécanisme de sécurité comme un code unique envoyé par courriel ou par texto à l'utilisateur. Elle complique l'accès sans autorisation aux systèmes de TI, car les pirates informatiques doivent alors posséder plusieurs éléments d'information ou appareils. Elle constitue aussi un moyen efficace d'accroître la sécurité et de protéger les données confidentielles contre les cybermenaces.

2.4 Comptes d'utilisateur privilégié ou superutilisateurs de la TI

Les membres du personnel de la TI disposent d'un compte d'utilisateur privilégié, également appelé compte de superutilisateur, dont ils se servent pour administrer et gérer les systèmes de TI. Ce compte leur donne habituellement un accès illimité aux données et aux autorisations propres à un système de TI. Ils s'en servent aussi pour apporter des changements aux systèmes de TI. À cet égard, il importe de contrôler l'accès aux comptes de superutilisateurs afin qu'on puisse suivre, surveiller et retracer les activités exécutées à l'aide de tels comptes, au besoin, notamment si une fraude est commise.

2.5 Attestation des comptes de TI privilégiés

En vertu de leur rôle, les employés ayant un accès privilégié aux TI peuvent ajouter, modifier ou supprimer des documents et des transactions, voire dans certains cas apporter des modifications aux journaux d'audit. Voilà pourquoi les organisations doivent contrôler ou restreindre l'accès aux comptes de superutilisateurs et passer en revue périodiquement l'accès des utilisateurs aux systèmes de TI afin que ce privilège soit réservé aux membres du personnel qui exécutent certaines fonctions professionnelles. En phase avec les pratiques exemplaires sectorielles, ces attestations doivent avoir lieu au moins une fois l'an ou dès qu'il y a un changement à l'effectif du service.

2.6 Journalisation des audits

Les journaux d'audit constituent des pistes générées par les systèmes et qui permettent de saisir, par ordre chronologique et dans le détail, les activités exercées par l'utilisateur d'un système de TI. On y trouve des activités telles que l'horodatage des ouvertures de session des utilisateurs, le type de données consultées,

les transactions modifiées ou supprimées ainsi que les anomalies ou exceptions décelées. Il est essentiel que les organisations autorisent la journalisation des audits en ce qui touche les incidents critiques dans les systèmes de TI afin qu'elles puissent établir l'obligation de rendre compte, repérer les modifications non autorisées aux données et déceler les activités frauduleuses.

2.7 Disponibilité des données – Rendement des systèmes de TI

Afin de réduire le risque de perturbation des activités opérationnelles en raison de pannes liées aux TI, les organisations doivent constamment faire le suivi du rendement des systèmes de TI. Le suivi des mesures de contrôle de la TI à l'aide de paramètres de rendement définis donne à la direction et aux équipes de la TI des points de repère leur permettant d'évaluer si le fonctionnement des systèmes de TI est à capacité optimale. Les paramètres en question s'étendent du suivi de la capacité du système de TI à l'application des rustines de sécurité en temps voulu, en passant par la sauvegarde réussie des données.

2.8 Suivi de la prestation des services

Les indicateurs de rendement clés (IRC) servent à jauger le service fourni. Ils jouent un rôle essentiel dans l'analyse du rendement et des avantages d'un actif de TI, comme les logiciels ou le matériel. Les organisations se servent des IRC et en font le suivi afin que le niveau de service attendu soit atteint.

2.9 Gestion des rustines

La mise en application de rustines de sécurité (ou de réglages de sécurité) à jour aux bases de données et systèmes de TI est cruciale. L'organisation pourra ainsi veiller à ce que les failles de la TI ne soient pas exploitées pour porter atteinte à la sécurité des données ou causer des pannes et à ce que les données confidentielles demeurent en sécurité.

La FPO a mis en place une norme de sécurité qui énumère les exigences relatives au mode et au stade de mise en application des rustines de sécurité aux failles liées à la cybersécurité.

La division de la cybersécurité du DGIFP est chargée de déceler les failles dans les bases de données et systèmes de TI. Cette tâche est réalisée au moyen d'un logiciel de sécurité qui scrute en temps réel (de façon continue) les bases de données et systèmes de TI pour y déceler les failles liées à la cybersécurité par rapport aux failles de notoriété publique que les fournisseurs et les experts en sécurité ont repérées.

Dès qu'une faille est décelée, la division de la cybersécurité en informe le groupement de TI afin que celui-ci puisse mettre en application les rustines de sécurité nécessaires, lesquelles peuvent également provenir du fournisseur. On attribue aux failles une cote de gravité selon une échelle allant de zéro à quatre en fonction du risque qu'elles surviennent et de leurs retombées éventuelles. La cote de gravité indique la rapidité avec laquelle il faut installer les rustines. À ce chapitre, le niveau d'urgence le plus élevé (dans les deux jours civils) correspond à la cote de gravité zéro et le plus bas (dans les 90 jours civils), à la cote de gravité quatre. Les groupements de TI sont responsables de la mise en application de ces rustines dans les délais prévus, suivant ce qui est décrit dans les Normes en matière d'information et de technologie du gouvernement de l'Ontario (NIT-GO).

2.10 Gestion des fournisseurs par groupement

Pendant que le DGIFP se charge de l'acquisition des biens et des services dont se sert l'ensemble de la FPO, les fournisseurs de TI qui assurent la prestation des services et du soutien ayant trait aux systèmes de TI utilisés par les ministères sont directement mis à contribution par leurs groupements de TI respectifs. La gestion des fournisseurs quant à la prestation de biens et de services est effectuée au niveau de la mise à contribution ou du contrat en particulier par le ministère ou le groupement de TI qui est responsable du contrat.

3.0 Objectif et étendue de l'audit

Notre audit avait pour objectif de déterminer si les systèmes de technologie de l'information (TI) sélectionnés dans quatre des huit groupements de TI de la fonction publique de l'Ontario (FPO) comptaient des systèmes et des processus efficaces pour :

- que les données et les systèmes de TI des Ontariens grâce auxquels on assure la prestation de programmes et de services gouvernementaux cruciaux soient sécurisés et fiables, y compris l'utilisation restreinte de l'accès privilégié et son suivi pour empêcher l'accès sans autorisation aux systèmes d'information;
- que les systèmes de TI fassent l'objet d'un suivi performant, d'une utilisation à capacité optimale et d'une analyse en fonction de paramètres de rendement établis;
- que les systèmes et processus empêchent les groupements de TI de faire appel en double à des fournisseurs de TI qui assurent la prestation de services semblables, que les fournisseurs fassent l'objet d'un suivi performant afin que les services soient rendus dans le respect des principes d'économie et que des mesures correctives soient prises en temps voulu, si besoin est.

Dans la planification de notre travail, nous avons établi les critères qui allaient servir à l'atteinte de notre objectif d'audit. Ces critères (voir **l'annexe 1**) reposent sur un examen des lois, des politiques et des procédures applicables, des facteurs de risque de la TI, des études internes et externes, et des pratiques exemplaires. La haute direction des groupements de TI et le Bureau du directeur général de l'information pour la fonction publique (DGIFP) ont passé en revue notre objectif d'audit et les critères connexes pour ensuite convenir de leur pertinence.

Notre audit s'est déroulé de janvier à septembre 2023. Nous avons a obtenu une déclaration écrite de la direction indiquant que le 17 novembre 2023, elle nous avait transmis toute l'information qui avait été portée à sa connaissance et qui pouvait sensiblement influer sur les constatations ou la conclusion du présent rapport.

Nous nous sommes entretenus avec des dirigeants principaux de l'information (DPI), des membres du personnel de la TI et des parties prenantes dignes d'intérêt qui, dans les quatre groupements de TI, occupent divers postes afin de passer en revue leurs rôles et responsabilités dans la gestion des systèmes de TI dont ils sont responsables ainsi que les processus établis pour exécuter les programmes gouvernementaux. Nous avons passé en revue les modalités établies qui définissent les objectifs et le mandat des groupements.

Nous avons sélectionné un échantillon des systèmes névralgiques de TI dans les quatre groupements. Nous avons passé en revue les mesures de contrôle de sécurité comme la politique sur les mots de passe et les paramètres des mots de passe afin d'analyser l'adhésion et la conformité aux Normes en matière d'information et de technologie du gouvernement de l'Ontario (NIT-GO) et aux normes sectorielles de sécurité.

Nous avons passé en revue la liste d'accès au système pour évaluer si l'accès des superutilisateurs fait l'objet d'une distinction adéquate et est réservé au personnel autorisé. De plus, nous avons analysé la mise en place de mesures de contrôle par les groupements pour passer périodiquement en revue l'accès des superutilisateurs ainsi que la suppression de l'accès aux comptes inactifs, conformément aux NIT-GO.

Nous avons passé en revue les mesures de contrôle en place quant à la tenue des journaux d'audit des renseignements très confidentiels, notamment par le suivi de ces journaux d'audit et de la conservation, en phase avec les règlements de la FPO. Nous avons aussi passé en revue divers rapports sur les indicateurs de rendement clés des activités qui témoignent du rendement des systèmes de TI pour faire en sorte qu'ils soient utilisés à bon escient et que leur fonctionnement soit à capacité optimale. En outre, nous avons passé en revue les mesures de contrôle permettant de suivre l'évolution du rendement des fournisseurs de TI ainsi que les documents permettant d'analyser si les groupements s'échangeaient entre eux des rapports sur le rendement. Nous avons aussi évalué si les groupements travaillaient en collaboration et tiraient parti des contrats en vigueur avec les fournisseurs de TI

afin d'éviter le dédoublement et la redondance dans les services.

Nous avons mené nos travaux et présenté les résultats de notre examen conformément aux Normes canadiennes de missions de certification – Missions d'appréciation directe publiées par le Conseil des normes d'audit et d'assurance des Comptables professionnels agréés du Canada (CPA Canada). Nous avons également obtenu un niveau d'assurance raisonnable.

Le Bureau du vérificateur général de l'Ontario applique la Norme canadienne de contrôle qualité. De ce fait, il maintient un système exhaustif de contrôle qualité comprenant des politiques et des procédures documentées au sujet du respect des règles de conduite professionnelle, des normes professionnelles, ainsi que des exigences législatives et réglementaires applicables.

Nous nous sommes conformés aux exigences en matière d'indépendance et d'éthique du Code de déontologie de l'Institut des comptables agréés de l'Ontario, qui est fondé sur des principes fondamentaux d'intégrité, d'objectivité, de compétence professionnelle, de diligence raisonnable, de confidentialité et de conduite professionnelle.

Au-delà du champ d'application

L'audit en question ici n'a pas porté en particulier sur les fonctions centralisées de la TI à l'échelle de la FPO comme la cybersécurité, le processus de gestion globale des risques, l'obtention de services de parties traitantes en TI, les actifs en TI tels que les ordinateurs portables, les fournisseurs d'une valeur de plus de deux millions de dollars, ainsi que les ententes sur les niveaux de service et les paramètres névralgiques de rendement ayant trait aux incidents de TI. Ces thèmes ont été passés en revue dans le cadre de notre audit de l'optimisation des ressources de 2022 du Bureau du dirigeant principal de l'information pour la fonction publique.

Annexe : Critères d'audit

Données préparées par le Bureau de la vérificatrice générale de l'Ontario

1. L'accès privilégié aux systèmes névralgiques de la technologie de l'information (TI), d'une importante cruciale dans la prestation des programmes et services gouvernementaux, est restreint au personnel selon le principe du besoin de savoir afin de prévenir l'accès sans autorisation aux données personnelles et de nature délicate.

2. Les indicateurs de rendement des systèmes névralgiques de la TI, comme l'accessibilité des systèmes, l'utilisation de la capacité, l'état des rustines, le vieillissement et les périodes de panne des systèmes, sont établis, mesurés par rapport aux cibles et suivis de façon à superviser efficacement le rendement des systèmes.

3. Les contrats en vigueur conclus avec les fournisseurs de TI sont mis à profit avant d'obtenir les services de nouveaux fournisseurs pour éviter l'obtention en double de services, pendant que le rendement des fournisseurs fait l'objet d'un suivi.

4. Des mesures de contrôle sont en place pour empêcher l'obtention en double des services de fournisseurs de TI qui assurent la prestation des mêmes services et logiciels.

5. Les groupements passent constamment en revue le rendement des fournisseurs selon des critères établis.

Bureau du vérificateur général de l'Ontario

20, rue Dundas Ouest, bureau 1530
Toronto (Ontario)
M5G 2C2

www.auditor.on.ca

ISBN 978-1-4868-7524-5 (PDF)