Vérificateur général
MANITOBA

Rapport à l'Assemblée législative du Manitoba

Vieillissement des systèmes d'information

Rapport d'audit indépendant

Version du site Web

février 2022

Cette page a été laissée
blanche intentionnellement.

La traduction de ce rapport a été fournie par le Service de traduction du Manitoba. En cas d'incohérence, se reporter à la version anglaise.

Cette page a été laissée
blanche intentionnellement.

Table des matières

Cette page a été laissée
blanche intentionnellement.

Commentaires du vérificateur général

La province du Manitoba a recours à des systèmes d'information pour offrir une large gamme de services à la population, notamment des possibilités d'inscription ou d'enregistrement en ligne, des demandes dans le cadre de programmes et des paiements.

Ces systèmes d'information comprennent du matériel informatique comme des serveurs, des pare-feu, des commutateurs et des routeurs, ainsi que les logiciels qui fonctionnent sur ces appareils. À mesure que ces systèmes d'information prennent de l'âge, ils deviennent davantage sensibles aux risques, comme des pannes de système prolongées, une baisse de leur fiabilité et une augmentation des vulnérabilités en matière de sécurité. Des systèmes vieillissants peuvent également se révéler incapables de répondre aux besoins et aux attentes en constante évolution des Manitobains. Il est important de surveiller l'âge et la pertinence des systèmes d'information pour veiller à les remplacer ou à les mettre à niveau au besoin.

La province a toujours largement recours à des systèmes d'information vieillissants. Je suis préoccupé par les limites des facteurs utilisés pour déterminer les risques qu'engendre la poursuite de l'utilisation de ces systèmes. Faute de prendre en compte des facteurs de risques plus étendus, certaines des cotes de risque actuelles pourraient sous-estimer ou surestimer les risques, entraînant la prise de mesures inadéquates pour réduire les risques à un niveau acceptable.

Nous avons remarqué qu'il n'y a pas de surveillance centralisée des résultats de l'évaluation des risques des systèmes vieillissants. Il s'agit d'une occasion manquée de repérer les facteurs de risque à l'échelle de tous les ministères, et de permettre à la Province d'adopter une approche d'atténuation des risques à l'échelle du système.

Nous avons également constaté une participation limitée des ministères dans l'évaluation des risques liés aux systèmes qu'ils utilisent, et dans la vérification de l'exactitude des inventaires des systèmes. Puisque la responsabilité d'établir des plans d'action visant les risques incombe aux ministères, il est important que leurs intervenants participent au processus d'évaluation des risques. Un manque de participation des ministères peut entraîner l'adoption de plans d'action inappropriés et mener à des cotes de risques erronées.

J'aimerais remercier la Division de la technologie et de la transformation opérationnelle, ainsi que les dirigeants et le personnel des ministères ayant collaboré avec nous, pour leur coopération et leur aide. J'aimerais également saluer les membres de mon équipe d'audit pour leur dévouement et leur travail rigoureux.

Tyson Shtykalo, CPA, CA
Vérificateur général

Raison pour laquelle nous avons mené cet audit

- La province du Manitoba (la Province) a recours à des systèmes d'information qui l'aident à offrir une large gamme de services à la population, notamment des possibilités d'inscription ou d'enregistrement en ligne, des demandes dans le cadre de programmes provinciaux et des paiements.
- Des systèmes d'information vieillissants exposent la Province à des pannes de système prolongées, à une baisse de leur fiabilité et à une augmentation des vulnérabilités en matière de sécurité.

Objectif

Déterminer si les risques associés au vieillissement des systèmes d'information de la Province sont décelés et gérés de façon à réduire la probabilité de conséquences négatives pour leurs utilisateurs et les services offerts aux Manitobains.

Conclusion

Les risques associés au vieillissement des systèmes d'information de la Province ne sont pas décelés et gérés de façon à réduire la probabilité de conséquences négatives pour leurs utilisateurs et les services offerts aux Manitobains.

Notre rapport comprend 8 RECOMMANDATIONS.

Nos constatations

DÉTERMINATION DES ACTIFS

L'inventaire des systèmes d'information de la Province, utilisé pour évaluer les risques liés au vieillissement des systèmes, est incomplet et inexact.

ÉVALUATION ET SIGNALEMENT DES RISQUES LIÉS AU VIEILLISSEMENT DES SYSTÈMES

Le processus d'analyse et de signalement des risques liés aux systèmes vieillissants est inadéquat.

- Les normes de technologie de l'information et des communications (TIC), utilisées comme fondement des cotes de risques, ne sont pas maintenues à jour.
- L'âge des technologies de soutien et le nombre de personnes-ressources mises à disposition pour le soutien des applications sont les seuls facteurs pris en compte pour déterminer les risques liés aux systèmes vieillissants.
- Les risques qui subsistent après l'étude des contrôles et d'autres facteurs d'atténuation (les risques résiduels) ne sont pas pris en compte dans les cotes finales des risques.
- Les résultats ne sont pas présentés avec exactitude en raison d'erreurs.
- Les intervenants des ministères ne participent pas à la détermination finale des cotes de risque.

SURVEILLANCE CENTRALISÉE DES RISQUES ET DES MESURES

Il y a un manque de pratiques en place pour surveiller les cotes de risque des systèmes vieillissants, et les réponses à ces risques ne sont pas bien définies.

- Il n'y a pas de rapport combiné des cotes de risque et des réponses aux risques qui couvrent tous les ministères.
- Les rapports sur l'état des biens informatiques sont diffusés de manière limitée aux intervenants et fournissent des renseignements insuffisants sur les risques.
- Les rapports sur l'état des biens informatiques ne sont pas publiés en temps opportun.

Cette page a été laissée
blanche intentionnellement.

Contexte

La province du Manitoba (la Province) a recours à des **systèmes d'information** qui l'aident à offrir une large gamme de services à la population. Cela comprend des possibilités d'inscription ou d'enregistrement en ligne, des demandes dans le cadre de programmes provinciaux et le traitement de paiements relatifs à différents services, par exemple des services d'éducation, de santé ou sociaux. À mesure que de nouveaux systèmes d'information améliorent l'expérience des utilisateurs dans le secteur privé, les gens s'attendent à un niveau de service semblable de la part du secteur public, souvent hors des heures d'ouverture normales.

Pour les gouvernements, adopter de nouveaux systèmes d'information ou moderniser les systèmes vieillissants en place permet de créer des processus plus efficients et de disposer d'une plus grande flexibilité pour répondre aux besoins des utilisateurs. Adopter de nouveaux systèmes ou moderniser ceux qui sont en place est également susceptible de diminuer les coûts de fonctionnement, car les systèmes d'information vieillissants courent le risque d'une hausse de leurs frais de fonctionnement, en raison d'un plus grand nombre d'exigences d'entretien.

Un **système d'information** s'entend d'un ensemble de plusieurs composants, comme du matériel et des logiciels, participant à la collecte, au traitement, au stockage et à la diffusion de renseignements.

Une **retouche** est une correction d'une vulnérabilité ou d'un défaut dont la découverte est postérieure au lancement d'une application ou d'un logiciel.

Une **base de données** est un ensemble de renseignements ou de données organisé selon une structure, habituellement stocké sous forme électronique dans un système informatique.

Un **système d'exploitation** est un programme qui agit comme une interface entre le matériel informatique du système et l'utilisateur. On peut citer par exemple Microsoft Windows, macOS et Linux.

En outre, le vieillissement des systèmes d'information expose la Province à des risques comme des pannes de système prolongées empêchant la prestation de services, une baisse de leur fiabilité et des vulnérabilités pouvant être évitées en matière de sécurité, car les systèmes plus vieux pourraient ne plus être compatibles ou ne plus faire l'objet de **retouches**.

On peut classer ces systèmes d'information en applications opérationnelles ou en infrastructures de réseau partagé. Les applications opérationnelles sont des systèmes que les ministères utilisent à des fins d'opérations internes et de prestation de services à la population. Cela comprend les technologies de soutien, lesquelles sont composées des **bases de données**, des **systèmes d'exploitation** et des langages de programmation. Les infrastructures de réseau partagé sont des actifs qui ne sont pas nécessairement attribués à un ministère en particulier,

mais plutôt utilisés pour la prestation de services commune à tous les ministères, ou à plusieurs d'entre eux. Cela comprend des appareils comme, notamment, les pare-feu, les commutateurs, les routeurs et les serveurs.

La Division de la technologie et de la transformation opérationnelle (la Division) du ministère du Travail, de la Protection du consommateur et des Services gouvernementaux est responsable d'évaluer chaque année la santé technologique de tous les systèmes d'applications opérationnelles et de leurs technologies de soutien.

Les technologies de soutien sont consignées dans le système de gestion du portefeuille d'applications de TI de la Division. Celle-ci a développé ce système à l'interne afin de classer les biens informatiques et les technologies de soutien correspondantes. En outre, le nombre de personnes-ressources affectées au soutien des applications est également consigné dans ce système, car il s'agit également d'un facteur de risque pris en compte dans l'évaluation globale des risques techniques liés aux applications opérationnelles.

La Division évalue chaque technologie de soutien et lui attribue une cote en fonction de sa position dans le cycle de vie technologique selon les normes de technologie de l'information et des communications (TIC) de la Province. Chaque technologie de soutien obtient une cote relative à son risque : faible (verte), moyen (jaune) ou élevé (rouge) en fonction du point où elle en est dans son cycle de vie. Le tableau suivant résume la cote de risque utilisée pour chaque étape du cycle de vie (verte, jaune et rouge) et le nombre de personnes-ressources affectées au soutien des applications.

Cote de risque/ couleur attribuée	Étape du cycle de vie	Personne(s)-ressource(s) de soutien des applications
Faible/verte	Exploitation de base	Fournisseur; la Division (plus de deux personnes)
Moyen/jaune	Confinement	La Division (deux personnes)
Élevé/rouge	Fin de vie	La Division (une personne ou aucune)

Les étapes du cycle de vie sont définies dans les normes de TIC comme ci-dessous :

- **Exploitation de base** – concerne les technologies et les processus en cours d'utilisation par la Province du Manitoba et conformes aux normes de TIC. Ces technologies ont atteint un niveau de maturité acceptable et sont réputées rendre de bons services au gouvernement.
- **Confinement** – concerne les technologies et les processus qui devraient uniquement servir à des fins limitées (par exemple, la maintenance) ou qui sont nécessaires pour satisfaire à des besoins précis de prestation de services pour la Province, que l'on ne peut obtenir grâce aux éléments de l'exploitation de base. Cette cote signale également un stade où les nouveaux développements devraient être limités.

- **Fin de vie** – concerne les technologies et les processus dont la Province a décidé la fin de l'exploitation et qui ne devraient pas être utilisés dans le cadre de développements en cours ou à venir. Il s'agit de technologies qui ont atteint la fin de leur cycle de vie.

Après avoir attribué une cote à chaque technologie de soutien, le système de gestion du portefeuille d'applications de TI calcule la cote globale de risque technique pour chaque application opérationnelle en déterminant le facteur de risque le plus élevé. Par exemple, si toutes les technologies de soutien et les soutiens des applications ont une cote de risque verte, la cote finale sera verte. Mais si un seul d'entre eux a une cote de risque jaune ou rouge, la cote finale deviendra elle aussi jaune ou rouge. En conséquence, il est nécessaire de veiller à la mise à jour des normes de TIC afin qu'elles suivent l'évolution rapide des technologies. Certaines technologies jugées comme assurant une exploitation de base il y a quelques années pourraient devoir être adaptées ou mises à jour aujourd'hui pour correspondre à une autre étape de leur cycle de vie.

Après avoir attribué une cote à chaque application opérationnelle, la Division produit des rapports sur l'état des biens informatiques, lesquels sont envoyés aux différents ministères. Il s'agit d'évaluations à un moment précis visant à aider les ministères à déterminer les risques techniques associés à leurs systèmes d'information, et à fournir des renseignements à prendre en compte lorsque chaque ministère planifie sa demande en TI. En fonction de la tolérance au risque d'un ministère, la Division lui recommande la mise en œuvre de réponses, lesquelles pourraient comprendre l'arrêt de l'exploitation, la mise à jour ou le remplacement d'un système. La Division recommande également au ministère de réviser ses plans de continuité des activités ou de reprise après sinistre, afin de garantir que ces plans sont en place pour ses services indispensables. Les définitions des risques techniques sont résumées dans le tableau ci-dessous, ainsi que les mesures recommandées par la Division pour chaque cote de risque.

Catégorie	Description de la cote de risque	Mesures recommandées
Verte Niveau 1 (faible)	Les technologies de soutien qui composent ce système d'applications opérationnelles peuvent être gérées par la Division ou les fournisseurs tiers.	Tous les systèmes subissent parfois des pannes imprévues. Nous recommandons de réviser vos plans de continuité des activités et de reprise après sinistre, pour garantir qu'ils sont à jour et correspondent à votre tolérance au risque.

Jaune **Niveau 2 (moyen)**	Une ou plusieurs des technologies de soutien qui composent cette application opérationnelle courent actuellement le risque de connaître une panne prolongée ou une défaillance irréparable dans un avenir proche.	Si ce système est important pour vos activités, votre ministère devrait envisager sa mise à jour ou son remplacement. Un investissement additionnel dans ce système n'est pas conseillé, à moins qu'il ne vise précisément à améliorer sa fiabilité technique. **Nous recommandons** que votre ministère : • prépare une évaluation des risques et un dossier de décision informatique; • passe en revue et mette à l'essai ses plans de continuité des activités; • communique avec la Division pour demander des prévisions budgétaires sommaires en matière de mise à jour ou de remplacement, et les inclue dans le plan d'investissement et de demande informatique de votre ministère.
Rouge **Niveau 3 (élevé)**	Une ou plusieurs des technologies de soutien qui composent cette application opérationnelle courent actuellement le risque de connaître une panne prolongée de service ou une défaillance irréparable. En conséquence, ce système pourrait cesser de fonctionner de façon imprévue, et la Division pourrait ne pas être en mesure de rétablir le service; le soutien est assuré dans la mesure du possible seulement. Les correctifs de cybersécurité, les corrections de bogues et les mises à jour pourraient ne pas être disponibles. En cas de menace à la cybersécurité, ces applications opérationnelles pourraient être mises hors ligne sans préavis pour protéger les données et l'environnement informatique du gouvernement du Manitoba.	Si ce système est important pour vos activités, nous recommandons fortement à votre ministère sa mise à jour ou son remplacement. Un investissement additionnel dans ce système n'est pas conseillé, à moins qu'il ne vise précisément à améliorer sa fiabilité technique. **Nous recommandons fortement** que votre ministère : • prépare une évaluation des risques et un dossier de décision informatique; • communique immédiatement avec la Division pour demander des prévisions budgétaires sommaires en matière de mise à jour ou de remplacement, et les inclue dans le plan d'investissement et de demande informatique de votre ministère. • passe en revue et mette à l'essai ses plans de continuité des activités.

La Division supervise la gestion par Kyndryl (qui faisait partie d'IBM) de l'infrastructure de réseau partagé de la Province. Comme l'infrastructure de réseau partagée ne relève pas nécessairement d'un ministère en particulier, la cote de risque de ces systèmes d'information n'est pas couverte par les rapports sur l'état des biens informatiques. Au lieu de cela, Kyndryl fournit à la Division un rapport de fin de vie mensuel portant sur tous les actifs qu'elle gère, et indique leurs dates de fin de service ou de fin de soutien. La Division utilise ces renseignements pour déterminer quels actifs doivent être remplacés ou mis à jour, de la même façon qu'elle suit les normes de TIC pour déterminer la cote de risque technique des applications opérationnelles dans le rapport sur l'état des biens informatiques.

Objectif de l'audit

Cet audit visait à déterminer si les risques associés au vieillissement des systèmes d'information de la Province sont décelés et gérés de façon à réduire la probabilité de conséquences négatives pour leurs utilisateurs et les services offerts aux Manitobains.

Portée et approche

L'audit comprenait une inspection des documents, des procédures, des normes, des rapports et des autres documents relatifs aux processus d'analyse des risques liés aux systèmes d'information vieillissants de la Province. Nous avons eu des entretiens avec des intervenants et des responsables de processus clés au sein de la Division de la technologie et de la transformation opérationnelle (la Division) afin de comprendre les processus et les activités en place pour analyser et évaluer les risques liés à la poursuite de l'utilisation de systèmes d'information vieillissants. Nous avons noté que différents processus sont utilisés pour analyser les risques menaçant les divers types d'actifs que sont les applications opérationnelles et les infrastructures de réseau partagé.

En ce qui concerne les applications opérationnelles, nous avons inspecté des rapports sur l'état des biens informatiques pour un échantillon de ministères, et nous sommes entretenus avec des intervenants ministériels, comme les directeurs généraux des finances et les représentants des TI. Les ministères compris dans l'échantillon étaient les suivants :

- Agriculture
- Familles
- Justice
- Travail, Protection du consommateur et Services gouvernementaux
- Transport et Infrastructure

Nous avons examiné ces rapports pour comprendre la façon dont ils sont utilisés pour élaborer des mesures qui gèrent les risques liés au vieillissement des systèmes. Le présent audit n'a pas examiné le processus de planification de la demande annuelle en TI, lequel s'appuie sur le rapport sur l'état des biens informatiques.

Nous avons obtenu les rapports que la Division utilise pour évaluer l'âge de l'infrastructure de réseau partagé et nous sommes entretenus avec des membres du personnel de la Division afin de comprendre les activités effectuées à l'aide de ces rapports dans le cadre de l'analyse des risques. Comme pour les applications opérationnelles, nous n'avons pas examiné le processus de financement visant à remplacer ou à mettre à jour l'infrastructure de réseau partagé.

Critères d'audit

Pour effectuer le présent audit, nous avons utilisé les critères suivants :

	Critères d'audit	Source
1	Tous les systèmes devraient être déterminés afin d'évaluer les risques liés à leur vieillissement.	COBIT5 BAI09.01, BAI09.02; NIST *Cybersecurity Framework 1.1 – Asset Management* (ID.AM)
2	La province devrait avoir un processus en place pour déceler, analyser et signaler les risques liés aux systèmes vieillissants.	COBIT5 APO12.01, APO12.02, APO12.05; NIST *Cybersecurity Framework 1.1. – Risk Assessment* (ID.RA)
3	La province devrait disposer de pratiques visant à examiner et à évaluer les résultats de l'analyse des risques liés aux systèmes vieillissants et à prendre des mesures pour atténuer les risques à un niveau acceptable.	COBIT5 APO12.04, BAI04.02; NIST *Cybersecurity Framework 1.1. – Risk Management Strategy* (ID.RM)

La province ne détecte et ne gère pas adéquatement les risques relatifs aux systèmes d'information vieillissants

La province du Manitoba (la Province) a un processus en place pour évaluer les risques techniques liés aux applications opérationnelles et pour déterminer quelles infrastructures de réseau partagé doivent être remplacées ou mises à jour. Cependant, nous avons conclu que la Province ne gère pas les risques liés aux systèmes d'information vieillissants de manière à réduire la probabilité de conséquences négatives pour leurs utilisateurs et les services offerts aux Manitobains, en nous appuyant sur les constatations suivantes :

- L'inventaire des systèmes d'information utilisé dans les évaluations des risques liés aux systèmes vieillissants est incomplet et inexact **(SECTION 1)**.
- Le processus utilisé pour analyser et signaler les risques liés aux systèmes vieillissants est inadéquat **(SECTION 2)**.
- Il y a un manque de pratiques visant à surveiller les cotes de risque des systèmes vieillissants et les réponses à ces risques **(SECTION 3)**.

1 L'inventaire des systèmes d'information utilisé pour évaluer les risques liés aux systèmes vieillissants est incomplet et inexact

La première étape de l'évaluation des risques liés aux systèmes d'information vieillissants est de déterminer la totalité de ceux-ci. Ce n'est qu'une fois que tous les systèmes devant être protégés ont été recensés que les menaces les visant peuvent être déterminées et que l'on peut mettre en place des défenses et des mesures de protection. De plus, déterminer les actifs permet d'attribuer leur responsabilité et l'obligation de répondre à leurs risques.

La responsabilité de déterminer les applications opérationnelles de la Province et de recueillir des renseignements à leur sujet incombe à la Division de la technologie et de la transformation opérationnelle (la Division). La Division consigne les technologies de soutien et le nombre de personnes-ressources affectées au soutien des applications dans le système de gestion du portefeuille d'applications de TI. Les cotes de risque finales déterminées dans ce système sont ensuite transmises aux ministères dans le rapport sur l'état des biens informatiques.

En ce qui concerne les actifs d'infrastructure de réseau partagé, Kyndryl fournit à la Division un rapport de fin de vie chaque mois. Ce rapport mentionne tous les actifs gérés par Kyndryl et leurs dates de fin

de service ou de fin de soutien, que la Division utilise pour déterminer quels actifs d'infrastructure de réseau partagé doivent être remplacés.

Nous avons constaté que l'inventaire des systèmes d'information que la Division utilisait pour évaluer les risques liés aux systèmes vieillissants était incomplet et inexact.

1.1 L'inventaire des applications et des technologies de soutien est incomplet et inexact

Nous avons examiné un extrait des cotes de risque des technologies de soutien et des personnes-ressources affectées au soutien des applications de l'ensemble des ministères en date de mars 2021. Nous avons constaté que 209 applications opérationnelles ont une technologie de soutien indéterminée, car elles sont désignées comme étant « s. o. » ou « inconnue » ou comme une technologie non mentionnée dans les normes de TIC (il s'agit du total de colonnes grises pour le langage de programmation, la base de données et le système d'exploitation à la **FIGURE 2**). Ces cas dans lesquels les technologies de soutien n'ont pas été déterminées pourraient signifier que la cote de risque globale de ces applications opérationnelles est incorrecte, car l'un des facteurs contribuant à la cote de risque finale n'a pas été déterminé.

Nous avons également inspecté les rapports sur l'état des biens informatiques de mars 2020 pour un échantillon de cinq ministères. Nous pensions que ces rapports présenteraient un inventaire complet et exact des applications opérationnelles sous la responsabilité des ministères. En discutant avec les représentants de chaque ministère concerné (y compris les directeurs généraux des finances et les directeurs des TI), nous avons découvert des cas dans lesquels les rapports finaux présentaient un inventaire inexact des applications opérationnelles sous leur responsabilité. Nous avons constaté qu'aucune procédure d'examen n'est mise en place entre la Division et les ministères pour vérifier le caractère complet et exact des systèmes d'information avant la publication des rapports finaux. Il importe que l'inventaire des applications opérationnelles soit complet afin que les ministères soient au courant des risques liés à toutes leurs applications et puissent créer les plans d'action nécessaires et appropriés en fonction de leurs besoins.

Nous avons noté les erreurs suivantes dans les rapports sur l'état des biens informatiques pour tous les ministères de l'échantillon :

Agriculture

- 4 applications sur 40 avaient été retirées en fin de vie, mais étaient toujours comprises dans le rapport sur l'état des biens informatiques.

Familles

- 1 application avait été retirée en fin de vie, mais était toujours comprise dans le rapport sur l'état des biens informatiques;
- 4 applications sur 56 avaient été transférées vers d'autres ministères, mais étaient toujours comprises dans le rapport sur l'état des biens informatiques;

- 14 applications relevant du ministère n'étaient pas indiquées dans le rapport sur l'état des biens informatiques.

Justice

- 2 applications avaient été transférées depuis d'autres ministères, mais n'étaient pas comprises dans le rapport sur l'état des biens informatiques.

Travail, Protection du consommateur et Services gouvernementaux

- 1 application n'était pas comprise dans la liste des actifs.

Transport et Infrastructure

- 8 applications sur 41 étaient comprises dans le rapport sur l'état des biens informatiques alors qu'elles ne relevaient plus du ministère;
- 2 applications sur 41 avaient été remplacées, mais étaient toujours comprises dans le rapport sur l'état des biens informatiques;
- 15 applications relevant du ministère n'étaient pas indiquées dans le rapport sur l'état des biens informatiques.

Les rapports sur l'état des biens informatiques visent à fournir aux ministères une cote du risque technique à un moment précis. Cela signifie que la responsabilité de certains systèmes pourrait changer entre le moment où la Division commence à travailler sur ce rapport et celui où il est terminé et envoyé aux ministères. En outre, puisque les rapports sur l'état des biens informatiques ne comprennent que des systèmes soutenus par la Division, d'autres systèmes pourraient être exclus d'une évaluation complète des risques liés aux systèmes vieillissants. Ces inexactitudes peuvent être atténuées ou évitées si un processus d'examen collaboratif est instauré pour confirmer l'exactitude de l'inventaire des actifs en comparant ceux de la Division et des ministères avant la finalisation et la publication de ces rapports.

Recommandation 1

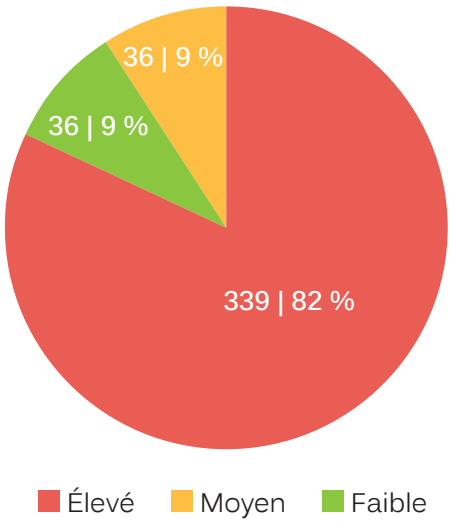
Nous recommandons que la Division mette en œuvre des mesures permettant de déterminer et de consigner avec exactitude l'intégralité des technologies de soutien et des applications opérationnelles dans le système de gestion du portefeuille d'applications de TI et les rapports sur l'état des biens informatiques.

2 Le processus utilisé pour analyser et signaler les risques liés aux systèmes vieillissants est inadéquat

Un processus de gestion des risques efficace permet aux intervenants d'évaluer la probabilité qu'un événement indésirable survienne et son incidence. Cette évaluation devrait être effectuée en utilisant des facteurs quantitatifs lorsqu'on peut disposer de données ou de mesures, et de facteurs qualitatifs lorsque ce n'est pas le cas. Le processus devrait également comprendre des étapes d'atténuation des risques lorsque des risques résiduels sont déterminés, et au besoin, appliquer des mesures d'atténuation supplémentaires, comme l'évitement, l'acceptation, le transfert ou la réduction des risques.

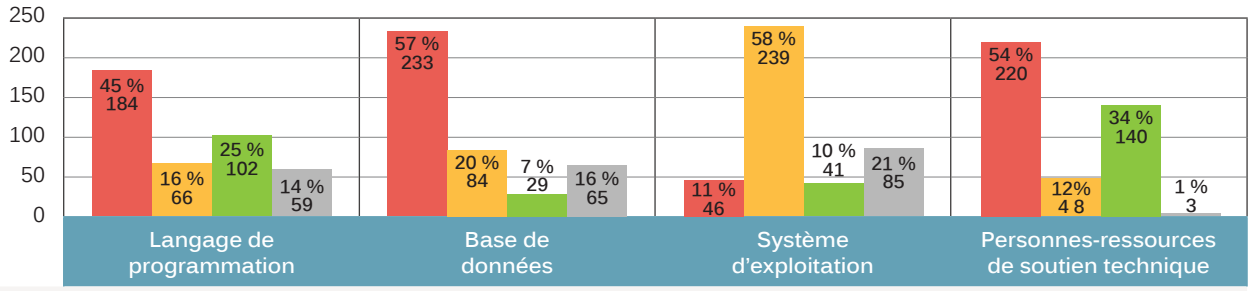
Le processus d'évaluation des risques actuel a démontré que sur 411 applications opérationnelles, 339 d'entre elles (82 %) avaient une cote de risque élevée (rouge) en mars 2021, comme l'illustre la FIGURE 1.

Figure 1 – Répartition de la cote de risque technologique pour les applications opérationnelles de l'ensemble des ministères en mars 2021



Ces cotes globales se fondent sur les évaluations des facteurs de risque de chaque application opérationnelle, ces facteurs comprenant les technologies de soutien et les personnes-ressources affectées au soutien des applications, comme l'illustre la FIGURE 2.

Figure 2 – Résumé des cotes de risques par facteur de risque (technologies de soutien et personnes-ressources affectées au soutien technique) pour tous les ministères en mars 2021



	Langage de programmation	Base de données	Système d'exploitation	Personnes-ressources de soutien technique
É	184	233	46	220
M	66	84	239	48
F	102	29	41	140
Grise	59	65	85	3
Total	411	411	411	411

Élevé Moyen Faible Grise

Ces cotes indiquent que de nombreuses applications opérationnelles et leurs technologies de soutien sont désuètes et devraient être remplacées, conformément aux recommandations de la Division. Comme le montre la **FIGURE 2**, 57 % des bases de données et 45 % des langages de programmation des applications (de type technologique) ont une cote de risque élevé. De plus, 54 % des applications opérationnelles nécessitent du personnel de soutien supplémentaire, car leur soutien se limite à une seule personne ou à aucune.

Selon les résultats actuels des cotes de risque, la Province a un nombre important de systèmes d'information vieillissants. La poursuite de leur utilisation augmente l'exposition à des risques comme des pannes prolongées, une baisse de la fiabilité des systèmes et une augmentation des vulnérabilités en matière de sécurité. Par ailleurs, nous avons constaté que le processus de détermination et de signalement des risques liés à la poursuite de l'utilisation des systèmes d'information vieillissants était inadéquat, tant pour les applications opérationnelles que pour les infrastructures de réseau partagé. En conséquence, certaines des cotes de risque actuelles pourraient être erronées (sous-estimées ou surestimées). Notre conclusion s'appuie sur les constatations suivantes :

- Les normes de technologie de l'information et des communications utilisées comme fondement de l'évaluation des systèmes n'ont pas été mises à jour **(SECTION 2.1)**.
- Les facteurs de risque pris en compte dans le processus actuel d'évaluation des risques des systèmes vieillissants se limitent à examiner à quel point les versions de chaque technologie de soutien sont à jour, et combien de personnes-ressources sont mises à disposition pour le soutien des applications **(SECTION 2.2)**.
- Les risques résiduels ne sont pas déterminés **(SECTION 2.3)**.
- Les ministères ne participent pas à l'évaluation des risques de leurs applications opérationnelles **(SECTION 2.4)**.
- Des cotes de risque inexactes ont été attribuées aux technologies de soutien dans le système de gestion du portefeuille d'applications de TI et les rapports sur l'état des biens informatiques présentaient des renseignements inexacts **(SECTION 2.5)**.

2.1 Les normes de TIC ne sont pas maintenues à jour

Les normes de TIC, sur lesquelles s'appuient les cotes de risque de chaque technologie de soutien, ont été mises à jour pour la dernière fois en avril 2019. Puisque la cote de risque technique se fonde sur la conformité des technologies aux normes de TIC, ce document doit être régulièrement mis à jour. Si l'évaluation des technologies de soutien se fonde sur des normes de TIC qui ne sont pas à jour, une technologie pourrait être évaluée comme en exploitation de base et recevoir une cote verte, alors qu'elle devrait déjà être considérée comme désuète et recevoir une cote de risque moyen (jaune) ou élevé (rouge).

Les normes de TIC déterminent le point où en est rendu un système d'information dans son cycle de vie technologique. Par conséquent, nous pensions que toutes les technologies de soutien consignées dans le système de gestion du portefeuille d'applications de TI correspondraient aux normes de TIC.

Cependant, nous avons découvert des cas où les technologies de soutien consignées dans le système de gestion du portefeuille d'applications de TI n'étaient pas mentionnées dans les normes de TIC. Cela signifie que les normes de TIC sont incomplètes et doivent être mises à jour pour représenter l'environnement technologique actuel de tous les ministères.

Recommandation 2

Nous recommandons :

a. que les normes de TIC soient mises à jour pour représenter toutes les technologies de soutien actuellement utilisées;
b. qu'un processus soit mis en place pour mettre à jour régulièrement les normes de technologie de l'information et des communications afin de suivre le rythme de l'évolution de la technologie.

2.2 Les facteurs de risque pris en compte sont limités

Nous avons constaté que les facteurs de risques utilisés pour déterminer le risque technique final des applications opérationnelles se limitaient à l'âge des technologies de soutien et au nombre de personnes-ressources mises à disposition pour le soutien des applications. Nous avons observé que seuls les renseignements sur la fin de vie fournis par le fournisseur sont utilisés pour évaluer les risques associés au vieillissement des infrastructures de réseau partagé.

Des facteurs qualitatifs et quantitatifs comme les suivants ne sont pas pris en compte pour estimer la cote globale de risque :

- Des critères quantitatifs ou mesurables pouvant fournir des données servant à calculer ou à déterminer le risque de façon objective, par exemple :
  - l'historique des pannes de système;
  - le nombre d'incidents consignés;
  - les indicateurs de rendement clé;
  - la durée de vie utile restante de l'actif;
  - les dépenses de fonctionnement.
- Des critères qualitatifs offrant une analyse plus subjective du risque, par exemple :
  - la fiabilité du système;
  - la capacité de satisfaire aux besoins du ministère;
  - la probabilité qu'un risque survienne;
  - les conséquences potentielles si un risque se réalise.

Comme les facteurs de risque sont limités, cela pourrait entraîner une évaluation inexacte des risques, ce qui pourrait signifier que les cotes de risque actuellement attribuées aux applications opérationnelles sont erronées. La limitation des facteurs de risque empêche également les intervenants comme la Division ou les ministères d'avoir une vision complète des risques liés aux systèmes d'information vieillissants affectant les applications opérationnelles.

2.3 Les risques résiduels ne sont pas déterminés

L'une des bonnes pratiques de l'évaluation des risques consiste à déterminer les contrôles et les autres facteurs d'atténuation pouvant réduire les menaces à des niveaux acceptables (c.-à-d. à des « risques résiduels »). Ces facteurs d'atténuation pourraient être les contrôles et les activités du processus opérationnel en place, ou bien des projets entrepris par la Division ou les ministères pour gérer les risques.

À l'heure actuelle, aucun mécanisme ne consigne les mesures correctives ou l'état de correction. Le rapport sur l'état des biens informatiques indique aussi explicitement qu'il ne comprend pas de renseignement sur l'état des mesures correctives pouvant être en cours. Il est important que la Division suive la trace de ces mesures et les surveille afin de déterminer si leur achèvement permet d'atténuer ou de réduire les risques à un niveau acceptable situé dans les limites de tolérance au risque. En surveillant étroitement ces activités, la Division aura la possibilité d'effectuer une évaluation complète des risques grâce à sa détermination et sa consignation de ces facteurs d'atténuation, de déterminer les risques résiduels et de prendre les mesures supplémentaires nécessaires pour répondre aux risques.

Recommandation 3

Nous recommandons l'utilisation de risques et de facteurs d'atténuation supplémentaires pour évaluer les risques liés aux systèmes d'information vieillissants, afin de repérer toutes les menaces et de déterminer les mesures nécessaires pour réduire ces menaces à des niveaux acceptables.

2.4 Aucun ministère ne participe à l'évaluation des risques

La Division affecte à ses systèmes des architectes et des analystes des activités pour réaliser les cotes de risque de ses applications opérationnelles. Ces personnes sont considérées comme des experts en la matière, en raison de leur participation au développement et à la maintenance de ces applications. Nous avons observé que les intervenants des ministères, comme les personnes qui utilisent ou gèrent les systèmes, ne participent pas à la détermination des cotes de risque, et ne reçoivent que la version finale du rapport sur l'état des biens informatiques.

Comme nous l'avons indiqué à la Recommandation 3, des facteurs de risque supplémentaires, comme la fiabilité du système et la capacité de satisfaire aux besoins du ministère, devraient être utilisés pour déterminer les cotes de risque des applications opérationnelles. Puisque les intervenants des ministères sont les premiers utilisateurs des systèmes, ils sont en mesure de procurer une rétroaction et des données essentielles pouvant être entrées dans ces facteurs de risque et dans l'évaluation globale des risques.

En outre, étant donné que ces ministères doivent mettre en œuvre des mesures pour répondre aux risques indiqués dans le rapport sur l'état des biens informatiques, il est important qu'ils participent au processus d'évaluation des risques. Les ministères doivent comprendre les motifs de la cote finale de risque technique pour déterminer et mettre en œuvre des plans d'action raisonnables visant à gérer ces risques.

Recommandation 4

Nous recommandons que la Division collabore avec les ministères pour évaluer les risques liés aux biens informatiques afin d'assurer que leurs connaissances directes soient prises en compte dans le cadre d'une évaluation complète des risques liés aux systèmes vieillissants.

2.5 Les cotes et la présentation des résultats comportent des inexactitudes

Nous avons constaté qu'il n'y a pas de contrôle des entrées lors de la consignation des technologies de soutien dans le système de gestion du portefeuille d'applications de TI. Aucun contrôle d'édition ni de validation ne permet d'empêcher les entrées erronées. Il n'y a pas non plus de processus d'examen rigoureux qui permettrait de détecter les inexactitudes. Nous avons constaté que certaines technologies de soutien n'avaient pas la cote de risque qui leur convenait lorsque nous avons comparé un extrait des cotes du risque du système de gestion du portefeuille d'applications de TI aux normes de TIC. Par exemple, une version du système d'exploitation Windows a obtenu une cote de risque moyen (jaune) dans le système de gestion du portefeuille d'applications de TI, alors que les normes de TI jugent qu'il est déjà en fin de vie et lui attribuent une cote de risque élevé (rouge). Cette évaluation inexacte d'une technologie de soutien pourrait entraîner la présentation d'une cote globale de risque inexacte dans le rapport sur l'état des biens informatiques, ou la prise de mauvaises mesures pour gérer ce risque. Dans cet exemple, la cote globale de risque n'a pas été affectée, car il était également considéré que le facteur lié aux personnes-ressources de soutien des applications présentait un risque élevé. Cependant, il est possible qu'aucune mesure ne soit prise pour gérer les risques liés au système d'exploitation.

Les rapports sur l'état des biens informatiques comprennent également des renseignements sur la capacité de reprise après sinistre. À mesure que les systèmes vieillissent, le risque qu'ils connaissent des défaillances augmente. La capacité de reprise après sinistre offre une assurance que les besoins

de continuité des services sont satisfaits et que les opérations essentielles sont préservées. Par conséquent, la Division recommande que les ministères examinent leur capacité de reprise après sinistre afin de garantir que leurs plans de reprise sont en place et peuvent être exécutés au besoin.

La Division nous a informés que certains ministères avaient déjà développé une capacité de reprise après sinistre pour leurs applications. Par exemple, le ministère des Familles dispose d'une capacité de reprise après sinistre pour une application opérationnelle. Toutefois, nous avons observé qu'aucune capacité de reprise après sinistre n'était en place sur un quelconque système dans les rapports sur l'état des biens informatiques des cinq ministères faisant partie de l'échantillon. Après avoir creusé la question auprès de la Division, nous avons été informés qu'il s'agissait d'une erreur qui devrait être corrigée. Cette erreur aurait pu avoir été détectée si les rapports avaient été contrôlés par les intervenants des ministères avant leur finalisation et leur publication.

Comme la Division s'attend à ce que les ministères utilisent les renseignements des rapports sur l'état des biens informatiques afin de décider des mesures nécessaires pour gérer les risques, elle doit s'assurer que ces rapports sont exacts et ne comportent pas d'erreur.

Recommandation 5

Nous recommandons que la Division mette en œuvre des méthodes permettant de garantir que le système de gestion du portefeuille d'applications de TI et les rapports sur l'état des biens informatiques ne comportent aucune erreur ou omission.

3 Manque de pratiques pour surveiller les cotes de risque des systèmes vieillissants et les réponses à ces risques

Les résultats de l'analyse des risques devraient être transmis aux intervenants affectés dans des formats aidant leur prise de décisions. Les décideurs devraient être informés des conséquences de l'utilisation continue de systèmes d'information vieillissants, de la probabilité que ces conséquences se réalisent et de l'incidence pour la Province. Le rapport sur les résultats de l'analyse des risques devrait également comprendre le profil de risque actuel, qui englobe l'efficacité des contrôles et des activités correctives en place, ainsi que l'état de correction.

Nous avons constaté que bien que des activités aient été mises en place afin de déterminer les risques techniques liés aux applications opérationnelles, les activités visant à surveiller les cotes de risques des systèmes vieillissants et les réponses à ces risques ne sont pas bien définies. Notre conclusion s'appuie sur les constatations suivantes :

- Il n'y a pas de rapport combiné des risques liés au vieillissement des systèmes et des réponses aux risques qui couvrent tous les ministères qui couvrent tous les ministères **(SECTION 3.1)**.

- Les rapports sur l'état des biens informatiques sont distribués à un public restreint et n'ont pas suffisamment de renseignements sur les cotes de risque pour soutenir les intervenants **(SECTION 3.2)**.
- Les rapports sur l'état des biens informatiques ne sont pas publiés en temps opportun **(SECTION 3.3)**.

3.1 Il n'y a pas de rapport combiné des cotes de risque et des réponses aux risques qui couvrent tous les ministères

Le **General Manual of Administration**, tel qu'approuvé le Conseil du Trésor, est la source autorisée de toutes les politiques et les procédures financières et administratives du gouvernement du Manitoba. L'article 5 de la Loi sur la gestion des finances publiques fournit le socle juridique de ce document.

Le **General Manual of Administration** établit la Division en tant qu'organisme principal de la Province en matière de gestion des TIC. Nous pensions donc que la Division agirait comme chef de file de la gestion des risques liés à l'utilisation continue de systèmes d'information vieillissants, notamment :

- en fixant des orientations stratégiques pour l'ensemble du gouvernement;
- en collaborant avec les ministères pour prendre des mesures afin d'atténuer ou de réduire les risques à des niveaux acceptables.

La Division a mis en œuvre des pratiques démontrant ses efforts dans ce sens, notamment en créant le rapport sur l'état des biens informatiques et ses procédures et lignes directrices connexes, ainsi qu'en ayant recours à un système de cotes de risque. La Division s'est assurée de procurer ces rapports sur l'état des biens informatiques aux ministères.

Cependant, nous avons constaté que la Division n'a pas préparé ni examiné un rapport de l'état des actifs combiné pour l'ensemble des ministères, résumant les cotes de risque de toutes les technologies de soutien, les applications opérationnelles et les infrastructures de réseau partagé. Ce rapport aurait fait ressortir les problèmes récurrents et les causes fondamentales et permettrait à la Division et aux ministères d'adopter une approche fondée sur le portefeuille d'applications pour répondre aux risques. Il pourrait également être utilisé pour surveiller les mesures prises ou planifiées afin de gérer les cotes de risques. En sa qualité d'organisme central qui gère les actifs de TIC de la Province, la Division connaît bien les technologies de soutien courantes utilisées dans l'ensemble des ministères, ainsi que les problèmes auxquels elles sont confrontées. En créant des solutions se fondant sur le portefeuille d'applications pouvant s'appliquer à plusieurs ministères, les plans de mesure d'atténuation des risques deviennent plus efficaces.

Recommandation 6

Nous recommandons que la Division prépare et examine un rapport d'évaluation des risques liés aux systèmes vieillissants combiné pour l'ensemble des ministères.

3.2 Les rapports sur l'état des biens informatiques ont une distribution limitée et fournissent des renseignements insuffisants sur les risques

La Division ne transmet les rapports sur l'état des biens informatiques qu'aux sous-ministres, aux sous-ministres adjoints et aux directeurs généraux des finances, par courriel. Les directeurs généraux des finances des ministères de l'échantillon examiné nous ont déclaré qu'ils pensaient ne pas pouvoir diffuser davantage les rapports sur l'état des biens informatiques. En effet, la Division indique explicitement dans ses courriels que les rapports ne doivent pas être redistribués, afin de protéger l'environnement technologique du gouvernement. Par conséquent, les chefs des TI des ministères, qui devraient être considérés comme des intervenants, ignorent les résultats des évaluations des risques techniques contenues dans les rapports sur l'état des biens informatiques. La confusion au sujet des personnes qui peuvent consulter les résultats des analyses des risques pourrait être évitée si des réunions étaient tenues entre les ministères et la Division, permettant de répondre aux questions sur la distribution des rapports et sur d'autres sujets et d'apporter des éclaircissements. Les directeurs généraux des finances des ministères de l'échantillon nous ont fait savoir qu'aucune réunion n'était organisée après l'envoi des rapports sur l'état des biens informatiques pour discuter de ceux-ci.

En outre, les rapports sur l'état des biens informatiques ne présentent que les cotes de risque technique de chaque application, et non une analyse des facteurs de risques servant à déterminer cette cote finale. Consulter ces détails serait profitable aux ministères, qui sont responsables de veiller au financement des actifs de TIC et de classer les projets de TIC par ordre de priorité. Grâce à ces renseignements, les ministères seraient en mesure de prendre des décisions pertinentes et éclairées quant au financement, et de collaborer avec la Division à l'élaboration de mesures d'atténuation des risques appropriées.

Recommandation 7

Nous recommandons que la Division tienne des rencontres avec les ministères pour :

a. déterminer le contenu approprié à inclure dans le rapport sur l'état des biens informatiques;
b. déterminer quels intervenants devraient recevoir le rapport sur l'état des biens informatiques;
c. discuter des résultats du rapport sur l'état des biens informatiques et collaborer à l'élaboration des mesures adéquates à prendre pour faire face aux risques.

3.3 Les rapports sur l'état des biens informatiques ne sont pas publiés en temps opportun

Le processus de réalisation de rapports sur l'état des biens informatiques a été élaboré en 2019 et fait partie du processus annuel de planification de la demande en TI. Ces rapports sont conçus pour aider les ministères à préparer des dossiers de décision afin de classer leurs projets de TI par ordre de priorité.

Chaque année, les ministères doivent présenter à la Division des dossiers de décisions avant une date précise. Nous avons constaté que les ministères n'avaient reçu les rapports sur l'état des biens informatiques de 2020 qu'après cette échéance. En conséquence, ils n'ont pas pu se servir de ces rapports pour étayer leurs dossiers de décisions relatifs au processus de planification des demandes en 2020. Cela pourrait mener les intervenants à conclure que les rapports sur l'état des biens informatiques sont inefficaces dans le cadre du processus de planification des demandes, et à diminuer l'importance de ceux-ci à leurs yeux.

Recommandation 8

Nous recommandons que la Division revoie le calendrier de préparation des rapports sur l'état des biens informatiques afin qu'il corresponde mieux au processus de planification de la demande en TI.

Renseignements supplémentaires sur l'audit

Ce rapport indépendant sur le vieillissement des systèmes d'information a été préparé par le Bureau du vérificateur général du Manitoba. Nous avions la responsabilité de fournir des renseignements objectifs, des conseils et une certification en vue d'aider l'Assemblée législative à surveiller la gestion des ressources et des programmes par le gouvernement et de conclure si les risques associés aux systèmes d'information vieillissants du gouvernement étaient décelés et gérés de façon à réduire la probabilité de conséquences négatives pour leurs utilisateurs et les services offerts aux Manitobains.

Tout le travail de cet audit a été exécuté à un niveau de certification raisonnable, conformément à la Norme canadienne de missions de certification (NCMC) 3001 – *Missions d'appréciation directe* établie par les Comptables professionnels agréés du Canada (CPA Canada) dans le Manuel de CPA Canada – Certification.

Le Bureau applique la Norme canadienne de contrôle qualité (NCCQ) 1 et, par conséquent, assure un système de contrôle de la qualité exhaustif, y compris des politiques et des procédures documentées concernant la conformité avec les règles de déontologie, les normes professionnelles et les exigences législatives et réglementaires applicables.

Pour effectuer notre travail d'audit, nous avons respecté les normes d'indépendance et les autres règles déontologiques du code de conduite professionnelle de l'Ordre des comptables professionnels agréés du Manitoba et le Code de valeurs, d'éthique et de conduite professionnelle du Bureau du vérificateur général du Manitoba. Tant les règles du code de conduite de l'Ordre des comptables que le Code du Bureau se fondent sur des principes fondamentaux d'intégrité, d'objectivité, de professionnalisme, de compétence et de diligence professionnelles, de confidentialité et de comportement professionnel.

Conformément à notre processus d'audit habituel, nous avons obtenu ce qui suit de la part de la direction :

1. la confirmation de la responsabilité de la direction quant à l'objet de l'audit;
2. la reconnaissance de la pertinence des critères utilisés pour l'audit;
3. la confirmation que tous les renseignements connus qui ont été demandés ou qui pourraient avoir une incidence sur les constatations ou la conclusion de l'audit ont été fournis.

Période couverte par l'audit

L'audit concernait la période allant de janvier 2019 à août 2021, période à laquelle se rapporte la conclusion de l'audit. Néanmoins, pour mieux comprendre l'objet de l'audit, nous nous sommes également penchés sur certains points qui ont précédé et suivi la période couverte par l'audit.

Date du rapport d'audit

Nous avons obtenu des éléments de preuve d'audit suffisants et appropriés sur lesquels fonder notre conclusion le 10 décembre 2021, à Winnipeg (Manitoba).

Cette page a été laissée
blanche intentionnellement.

Résumé des recommandations

Dans cette section, nous présentons un résumé de nos recommandations à la Division de la technologie et de la transformation opérationnelle et au ministère du Travail, de la Protection du consommateur et des Services gouvernementaux.

RECOMMANDATION 1

Nous recommandons que la Division mette en œuvre des mesures permettant de déterminer et de consigner avec exactitude l'intégralité des technologies de soutien et des applications opérationnelles dans le système de gestion du portefeuille d'applications de TI et les rapports sur l'état des biens informatiques.

Réponses des responsables :

La direction souscrit au principe de cette recommandation et évalue les options, le calendrier et les coûts en vue de développer et de mettre en œuvre des outils et des processus permettant de déceler et de consigner plus intégralement et avec plus d'exactitude les applications opérationnelles et les technologies de soutien dans le système de gestion du portefeuille d'applications et les rapports sur l'état des biens informatiques.

RECOMMANDATION 2

Nous recommandons :

a. que les normes de TIC soient mises à jour pour représenter toutes les technologies de soutien actuellement utilisées;
b. qu'un processus soit mis en place pour mettre à jour régulièrement les normes de technologie de l'information et des communications afin de suivre le rythme de l'évolution de la technologie.

Réponses des responsables :

La direction souscrit aux principes de ces recommandations et évalue les options, le calendrier et les coûts aux fins :

a. d'établir un processus annuel intégré de vérification de la santé des applications et des infrastructures, synthétisé dans le rapport sur l'état des biens informatiques;
b. d'établir un processus annuel de maintien d'un ensemble exhaustif de normes de TIC.

RECOMMANDATION 3

Nous recommandons l'utilisation de risques et de facteurs d'atténuation supplémentaires pour évaluer les risques liés aux systèmes d'information vieillissants, afin de repérer toutes les menaces et de déterminer les mesures nécessaires pour réduire ces menaces à des niveaux acceptables.

Réponses des responsables :

La direction souscrit au principe de cette recommandation et évalue les options, le calendrier et les coûts en vue de développer un ensemble plus exhaustif de facteurs de risque, conforme aux normes d'architecture des TI utilisées pour évaluer les systèmes aux fins du rapport sur l'état des biens informatiques.

RECOMMANDATION 4

Nous recommandons que la Division collabore avec les ministères pour évaluer les risques liés aux biens informatiques afin d'assurer que leurs connaissances directes soient prises en compte dans le cadre d'une évaluation complète des risques liés aux systèmes vieillissants.

Réponses des responsables :

La direction souscrit au principe de cette recommandation et évalue les options, le calendrier et les coûts en vue de développer et de mettre en œuvre un processus annuel d'évaluation des risques et des contrôles faisant participer les ministères afin d'évaluer les risques liés aux systèmes vieillissants et d'y répondre.

RECOMMANDATION 5

Nous recommandons que la Division mette en œuvre des méthodes permettant de garantir que le système de gestion du portefeuille d'applications de TI et les rapports sur l'état des biens informatiques ne comportent aucune erreur ou omission.

Réponses des responsables :

La direction souscrit au principe de cette recommandation et évalue les options, le calendrier et les coûts afin d'établir des processus qui tirent parti des nombreux mécanismes de vérification de l'inventaire et de leur statut, notamment les outils de détection automatique, la gestion des licences, les rapports des fournisseurs de services et les rapports internes dans le cadre de la préparation du rapport sur l'état des biens informatiques.

RECOMMANDATION 6

Nous recommandons que la Division prépare et examine un rapport d'évaluation des risques liés aux systèmes vieillissants combiné pour l'ensemble des ministères.

Réponses des responsables :

La direction souscrit au principe de cette recommandation et évalue les options, le calendrier et les coûts afin d'établir avec les ministères clients un processus d'examen permettant une évaluation de la santé des applications et des structures commune à l'ensemble du gouvernement.

RECOMMANDATION 7

Nous recommandons que la Division tienne des rencontres avec les ministères pour :

a. déterminer le contenu approprié à inclure dans le rapport sur l'état des biens informatiques;
b. déterminer quels intervenants devraient recevoir le rapport sur l'état des biens informatiques;
c. discuter des résultats du rapport sur l'état des biens informatiques et collaborer à l'élaboration des mesures adéquates à prendre pour faire face aux risques.

Réponses des responsables :

La direction prévoit :

a. déterminer le contenu approprié à inclure dans le rapport sur l'état des biens informatiques;
b. déterminer quels intervenants devraient recevoir le rapport sur l'état des biens informatiques;
c. discuter des résultats du rapport sur l'état des biens informatiques et collaborer à l'élaboration des mesures adéquates à prendre pour faire face aux risques.

RECOMMANDATION 8

Nous recommandons que la Division revoie le calendrier de préparation des rapports sur l'état des biens informatiques afin qu'il corresponde mieux au processus de planification de la demande en TI.

Réponses des responsables :

La direction évalue les options afin de synchroniser le processus d'évaluation de la santé pour que les rapports sur l'état des biens informatiques soient utilisés dans le processus de planification de la demande en TI (partie du processus de gestion du portefeuille d'applications).

Cette page a été laissée
blanche intentionnellement.

Notre vision

Être appréciés pour notre influence positive sur la performance du secteur public au moyen de travaux et de rapports d'audit aux effets importants.

Notre mission

Porter notre attention sur des domaines d'importance stratégique pour l'Assemblée législative et fournir aux députés de l'Assemblée des audits fiables et efficients.

Notre mission comprend la production de rapports d'audit faciles à comprendre qui incluent des discussions sur les bonnes pratiques au sein des entités verifiees et des recommandations que, une fois mises en œuvre auront des effets importants sur la performance du gouvernement.

Nos valeurs | Responsabilité | Intégrité | Confiance | Collaboration | Innovation | Croissance professionnelle

Vérificateur général
Tyson Shtykalo

Directeur général d'audits de technologies de l'information et de l'innovation
Wade Bo-Maguire

Responsable de l'audit informatique
Ian Montefrio

Gestionnaire des communications
Frank Landry

Soutien administratif
Jomay Amora-Dueck
Tara MacKay

Conception graphique
Waterloo Design House

Version du site Web

Vérificateur général
MANITOBA

Pour plus de renseignements, veuillez communiquer avec notre bureau :

Bureau du vérificateur général
330, avenue Portage, bureau 500
Winnipeg (Manitoba) R3C 0C4

Téléphone : 204 945-3790 Télécopieur : 204 945-2169
contact@oag.mb.ca | www.oag.mb.ca

Facebook.com/AuditorGenMB
Twitter.com/AuditorGenMB
Linkedin.com/company/manitoba-auditor-general