Emploi et Développement social Canada
Employment and Social Development Canada

Canada

Audit de la planification de la continuité des activités de technologies de l'information

Rapport

Mars 2022

Audit de la planification de la continuité des activités de technologies de l'information

Vous pouvez télécharger cette publication en ligne sur le site canada.ca/publicentre-EDSC.

On peut aussi obtenir ce document sur demande en médias substituts
(gros caractères, braille, audio sur CD, fichiers de texte sur CD
ou DAISY) en composant le 1 800 O-Canada (1-800-622-6232).
Si vous utilisez un téléscripteur (ATS), composez le 1-800-926-9105.

PDF
Nº de cat. Em20-158/2022F-PDF
ISBN : 978-0-660-43641-8

TABLE DES MATIÈRES

1. CONTEXTE

1.1 Contexte

L'audit de la planification de la continuité des activités de technologies de l'information (TI) a été inclus dans le plan d'audit en fonction du risque de 2019-2020 du ministère.

Emploi et Développement social Canada (EDSC) a versé plus de 120 milliards de dollars en prestations l'an dernier dans le cadre d'une vaste gamme de programmes et de services, dont la Sécurité de la vieillesse (SV), le Régime de pensions du Canada (RPC), l'assurance-emploi et le Programme canadien de prêts aux étudiants. La progression de la pandémie de COVID-19 a entraîné le déploiement d'autres programmes de prestations d'envergure, comme la Prestation canadienne d'urgence, la Subvention salariale d'urgence du Canada et la Prestation canadienne d'urgence pour les étudiants.

Ces programmes et services essentiels à la mission reposent sur des solutions de TI mises en œuvre, exploitées et tenues à jour par la Direction générale de l'innovation, de l'information et de la technologie (DGIIT) (en ce qui a trait aux applications et bases de données) avec le soutien de Services partagés Canada (SPC) (en ce qui a trait aux plateformes et à l'infrastructure).

À EDSC, les pratiques et les activités qui assurent le rétablissement des solutions de TI sont appelées activités de reprise après sinistre (RS) appuyées par des plans de reprise technique. Ces activités et les plans connexes sont gérés par la Division de la gestion de la dette technique/continuité des activités de TI de la Direction de la durabilité des activités opérationnelles au sein de la DGIIT.

Le groupe Gestion des urgences et continuité des activités, qui relève du dirigeant principal de la sécurité au sein de la Direction générale des services d'intégrité (DGSI), coordonne les activités de gestion de la continuité des opérations (p. ex. l'élaboration de stratégies de continuité des activités) avec les directions générales et les régions afin d'assurer la préparation de l'ensemble du ministère et de ses composantes en vue du maintien des activités en cas de perturbation ou de catastrophe. Bien que la planification de la continuité des activités de TI soit explicitement liée à la stratégie de continuité des activités dans le cadre de chaque programme ou service ministériel, elle constitue un sous-ensemble clé de la planification de la continuité des activités (PCA).

1.2 Objectif de l'audit

L'objectif de l'audit était d'évaluer les activités de gouvernance, de gestion des risques et de gestion des programmes liées à la planification de la continuité des activités de TI qui portent sur la disponibilité continue des applications essentielles aux programmes et aux services ministériels.

1.3 Portée

Parmi les 19 plans de reprise technique en place couvrant plus de 122 solutions à l'appui des programmes ministériels essentiels à la mission, l'équipe d'audit a choisi quatre (4) plans qui couvrent 89 solutions appuyant des opérations à impact important, aux fins d'évaluation. Cet échantillon a été jugé le plus représentatif, car il comprenait des plans couvrant un grand nombre d'utilisateurs internes et externes et de solutions. Les plans de reprise technique visés sont les suivants :

- Plan de reprise technique du RPC des systèmes de la charge de travail relative aux pensions (SCTP)
- Plan de reprise technique du Guichet-Emplois
- Plan de reprise technique du programme d'assurance-emploi pour les services de cyberauthentification d'entreprise (SCE), Mon dossier Service Canada (MDSC), Mon dossier d'entreprise Service Canada (MDESC) et le relevé d'emploi (RE) - Traitement automatisé des demandes (TAD) en ligne
- Plan de reprise technique du programme d'assurance-emploi des ordinateurs centraux Unisys

L'audit a été effectué entre septembre 2021 et octobre 2021.

L'audit excluait les secteurs sous la responsabilité de SPC (p. ex. la reprise au niveau de l'infrastructure sur laquelle les solutions sont hébergées, des centres de données). Il excluait également la PCA puisque cette évaluation a été effectuée dans le cadre d'un audit précédent.

1.4 Méthodologie

Avec l'aide de professionnels contractuels, l'audit a été réalisé selon les méthodes suivantes :

- Examen et analyse de la documentation ;
- Entrevues avec des membres de la DGIIT et de la DGSI.

Les composantes de la planification de la continuité des activités de TI ont été évaluées en fonction d'un ensemble d'outils et de ressources connus et recommandés, notamment :

- Politique sur la sécurité du gouvernement de 2019 du Secrétariat du Conseil du Trésor
- Agence fédérale de gestion des urgences (FEMA) du département de la Sécurité intérieure des États-Unis
- Cadre de sécurité civile pour le Canada de 2017 de Sécurité publique

- Directives de l'Information System Audit and Control Association (ISACA®), y compris les Control Objectives for Information and related Technology (COBIT®), version 4.1, du cadre de l'IT Governance Institute® (ITGI™)

2. CONSTATATIONS DE L'AUDIT

2.1 Cadre de continuité des activités de TI

Un cadre de continuité des activités de TI est un sous-ensemble du processus de gestion de la continuité des activités à l'échelle de l'organisation. Le cadre exige qu'une analyse des répercussions sur les activités (ARA) soit effectuée et que des plans de reprise technique soient élaborés. De plus, le cadre établit une stratégie pour permettre au ministère d'intervenir en cas d'incidents et de perturbations afin de poursuivre l'exploitation des processus de programmes essentiels pour maintenir la disponibilité des services et de l'information à un niveau acceptable.

Il n'existe pas de cadre stratégique défini décrivant la feuille de route ministérielle relative à la continuité des activités de TI

La directive relative à la gestion de la continuité des activités d'EDSC est conforme à la directive sur la gestion de la sécurité du Secrétariat du Conseil du Trésor et donne un aperçu de la gouvernance, des rôles et des responsabilités. Toutefois, aucun cadre stratégique défini n'est en place pour la continuité des activités de TI.

En l'absence d'une stratégie de continuité des activités de TI dûment réalisée et approuvée, il existe un risque que les plans de reprise technique et la PCA soient incohérents et désalignés, ce qui pourrait faire en sorte que le ministère ne soit pas en mesure de réagir aux incidents et aux perturbations de manière exhaustive, efficace et reproductible.

Les processus de création, de tenue à jour et de mise à l'essai des plans de reprise technique ne sont pas évolués

Bien que des données probantes indiquent que la plupart des éléments nécessaires pour un cadre de continuité des activités de TI existent (par exemple la création de plans de reprise technique, la mise à l'essai de l'infrastructure ou des plateformes hébergeant les solutions d'EDSC), l'audit a révélé que les processus sont ponctuels plutôt que définis.

En outre, l'audit a révélé que les plans de reprise technique ne suivent pas une approche commune et structurée tant du point de vue du contenu que du point de vue de la portée. Par exemple, certains plans couvraient des solutions uniques tandis que d'autres couvraient jusqu'à 70 solutions.

Il existe un risque que les contrôles soient manquants ou ne soient pas documentés adéquatement, ce qui pourrait nuire à la capacité de l'organisation d'effectuer systématiquement des activités de RS et d'évaluer leur efficacité et d'apporter des ajustements au besoin.

Depuis la mise en place de l'équipe responsable de la continuité des activités de TI en 2019, rien n'indique que des plans de reprise technique ont été présentés aux comités de gouvernance

Bien que des progrès relatifs aux activités de RS soient signalés à des organismes de gouvernance comme le Comité d'examen de l'architecture et le Comité consultatif des directeurs généraux, l'audit a révélé que les présentations portaient sur la complexité de l'infrastructure et de la dette technique plutôt que sur la continuité des solutions ministérielles.

Sans le dépôt, l'examen et l'approbation officiels des plans de reprise technique par les responsables de la gouvernance, la compréhension et l'acceptation des activités, des processus, des rôles et des responsabilités pourraient être déficientes et présenter un risque pour la mise en œuvre efficace du cadre. De plus, en l'absence d'un examen de la gouvernance des plans de reprise technique, il y a un risque que la surveillance et la prise de décisions nécessaires pour régler les incidents ou les perturbations ne soient pas claires et soient difficiles à exécuter.

Recommandations

1. La DGIIT devrait définir un plan stratégique ministériel relatif à la continuité des activités de TI selon les exigences de la planification de la continuité des activités du ministère et documenter les processus liés au cadre.
2. La DGIIT devrait inclure le cadre et les plans de continuité des activités de TI présentés aux comités de gouvernance aux fins d'approbation et pour confirmer l'harmonisation entre les résultats de l'analyse des répercussions sur les activités, les plans de reprise technique et la gestion de la continuité des activités à l'échelle de l'organisation, les priorités ministérielles essentielles et les initiatives stratégiques.

Réponse de la direction

1. La DGIIT est d'accord. Les mesures devraient être prises d'ici mars 2023.

2. La DGIIT est d'accord. Les mesures devraient être prises d'ici septembre 2022.

2.2 Gestion des risques

Une ARA permet de déterminer les conséquences de la perturbation d'une fonction ou d'un processus opérationnel et de recueillir les renseignements nécessaires pour élaborer des stratégies de reprise. Les scénarios de pertes potentielles sont déterminés lors de l'évaluation des risques. Une ARA est une évaluation qui met l'accent sur les répercussions opérationnelles et qui détermine l'objectif de temps de reprise (OTR) pour fournir des lignes directrices concernant le temps requis pour la reprise ou fournir des services provisoires, ainsi que l'objectif de point de rétablissement (OPR) pour fournir des lignes directrices au sujet de l'interruption ou de la perte maximale tolérable concernant les données.

Des ARA opérationnelles et techniques distinctes sont actuellement créées pour chaque programme ou plan de reprise technique

L'audit a permis de constater que la DGIIT reconnaît qu'il existe actuellement deux processus d'élaboration d'ARA et que les OTR et les OPR sont déterminés à deux endroits : ARA des TI et ARA de programmes. Selon la DGIIT, les ARA des TI ont initialement été élaborées pour remédier à l'absence d'ARA de programmes. Comme cette lacune a maintenant été comblée et que la DGSI crée des ARA de programmes dans le cadre d'un processus reproductible, la DGIIT n'en produira plus.

Jusqu'à ce qu'un examen complet des ARA des TI soit effectué et que celles-ci soient éliminées, il existe un risque que deux ARA en place entraînent des incohérences, un décalage et des retards pour établir un seul OTR et un seul OPR.

Les documents d'ARA ne sont pas systématiquement mis à jour

En ce qui concerne les activités d'ARA des TI, parmi les quatre plans de reprise technique couvrant 89 solutions critiques qui ont été échantillonnés, une seule solution critique a fait l'objet d'une ARA. Toutefois, en ce qui concerne les ARA de programmes, l'équipe d'audit a pu obtenir des ARA relatives à des programmes particuliers qui visaient des solutions critiques, et celles examinées étaient complètes et à jour. La DGIIT prévoit mettre fin à l'exécution d'ARA des TI, dans la mesure où des ARA de programmes sont déjà disponibles. Cela atténuerait le risque d'élaborer des ARA en double, ce qui pourrait entraîner des incohérences, un décalage et des retards pour établir un seul OTR et un seul OPR.

Recommandation

3. La DGIIT devrait tirer parti d'une évaluation à jour unique des répercussions sur les activités qui tiendrait compte des OTR et des OPR pour toutes les solutions critiques.

Réponse de la direction

3. La DGIIT est d'accord. Les mesures devraient être prises d'ici mars 2023.

2.3 Plans de reprise technique

On prévoit que la DGIIT élaborera des plans qui feront partie du cadre de continuité des activités de TI pour répondre aux exigences en matière de continuité des activités définies dans la PCA du ministère. On prévoit également que la DGIIT maintiendra des plans de continuité des activités de TI pour tenir compte des changements et des modifications apportés aux solutions et aux systèmes dans le cadre de la PCA du ministère. En outre, les plans devraient faire l'objet d'une mise à l'essai périodique, y compris une vérification complète des processus de continuité et des exercices de mise en situation visant à vérifier les hypothèses et les procédures de rechange définies dans les plans.

Des éléments clés sont omis dans les plans de reprise technique

L'audit a révélé que, dans l'ensemble, 11 % des plans de reprise technique en place ne

comportent pas les coordonnées des ressources techniques, ce qui pourrait nuire à la capacité de communiquer avec le personnel en cas d'interruption du service. En outre, certains plans (p. ex. plans couvrant le dossier d'antécédents d'emploi — DAE et le système ministériel de gestion des paiements [SMGP] — solutions du SMGP) ne comportent pas de composantes essentielles (p. ex. stratégie de reprise, diagrammes architecturaux, etc.), ce qui pourrait entraîner une interruption prolongée en cas d'incidents ou de perturbations.

Les plans ne sont pas tenus à jour en temps opportun

L'audit a révélé que 89 % des plans de reprise technique sont échus, la date d'expiration la plus ancienne remontant à 2018. La DGIIT a élaboré un calendrier de mise à jour des plans de reprise technique désuets qui est lié aux activités d'essais de RS en cours ou prévues.

Les plans désuets pourraient entraîner un risque de ne pas être en mesure de joindre le personnel ainsi que des références inexactes aux services techniques, ce qui entraînerait des interruptions prolongées des activités.

Les activités d'essais ne sont pas à jour

L'audit a révélé qu'un processus est en place pour vérifier les solutions dans le cadre de la mise à l'essai du plan de continuité de l'infrastructure menée par SPC. Lorsqu'un essai est prévu (y compris des exercices sur table), une demande de changement est soumise à l'approbation des intervenants techniques et opérationnels au niveau du directeur général.

Les personnes interrogées ont révélé que de récentes activités d'essais ont été menées pour quelques solutions, par exemple les essais fonctionnels effectués en ce qui concerne les solutions relatives aux ordinateurs centraux pour le RPC et la SV. De plus, les personnes interrogées ont révélé que des leçons apprises sont produites pour les solutions mises à l'essai et utilisées pour améliorer les futures activités d'essais.

Un calendrier qui met en évidence les plans futurs en matière d'essais a été élaboré. On a fourni des preuves qui montrent que des responsables fonctionnels ont été engagés pour communiquer les dates d'interruption et approuver les créneaux horaires d'essai. Toutefois, aucun indicateur de rendement clé n'est établi pour permettre la production de rapports sur l'efficacité des essais.

Recommandations

4. La DGIIT devrait confirmer que les plans de reprise technique :
    a. comprennent les rôles, les responsabilités et les obligations redditionnelles ;
    b. sont définis, documentés, communiqués et revus périodiquement ;
    c. tiennent compte globalement des parties internes et externes, y compris les partenaires et les fournisseurs ;

d. assurent la validité des détails (services, solutions, coordonnées des personnes-ressources, etc.) ;

e. sont examinés pour vérifier qu'ils sont complets et qu'ils comprennent des sections clés comme une stratégie de reprise et des diagrammes d'architecture.

5. La DGIIT devrait élargir la portée des essais pour inclure l'ensemble de la solution (essais fonctionnels, essais de production et exercices sur table) afin de permettre un meilleur état de préparation du programme en cas de sinistre et d'obtenir des scénarios d'essai qui reflètent un scénario de reprise réelle.

6. La DGIIT devrait établir des indicateurs de rendement clés pour rendre compte de la pertinence des essais.

Réponse de la direction

4. La DGIIT est d'accord. Les mesures devraient être prises d'ici juillet 2022.

5. La DGIIT est partiellement d'accord, la Méthodologie existante de test de continuité des TI fournit le cadre pour les tests de solutions entières lorsque cela est possible. Cependant, il existe des limitations dans les environnements de centres de données patrimoniaux qui empêchent les tests de production de solutions entières. Les mesures devraient être prises d'ici mars 2023.

6. La DGIIT est d'accord. Les mesures devraient être prises d'ici septembre 2022.

3. Conclusion

L'audit a permis de conclure que, dans l'ensemble, sans la mise à l'essai des plans de reprise technique, on ne peut pas établir clairement si les plans fonctionneront comme prévu en cas de perturbation ou de sinistre.

Au niveau de la gouvernance, diverses activités de RS sont signalées aux organismes de gouvernance. Toutefois, les exigences en matière de rapports et les mécanismes des plans de reprise technique selon un cadre défini de continuité des activités de TI n'existent pas ou ne permettent pas la surveillance et l'approbation opportunes des processus.

Du point de vue de la gestion des risques, il est possible de rationaliser le processus d'ARA pour assurer la cohérence et l'harmonisation avec le programme global de PCA.

Il existe une marge de manœuvre pour améliorer la gestion des plans de reprise technique en place. Plus précisément, un mécanisme de maintien des plans au moyen d'un examen courant n'est pas en place. La DGIIT va dans la bonne direction alors qu'elle a élaboré un calendrier de maintien des plans qui est lié aux activités d'essais de RS en cours.

4. Déclaration d'assurance

Selon notre jugement professionnel, les procédures d'audit appliquées et les éléments probants recueillis sont suffisants et appropriés pour appuyer l'exactitude des conclusions présentées dans le présent rapport. Ces conclusions sont fondées sur les observations et les analyses faites lors de l'audit. Les conclusions s'appliquent uniquement à l'audit de la planification de la continuité des activités de TI. Les éléments probants ont été recueillis conformément à la *Politique sur l'audit interne* du Conseil du Trésor et aux *Normes internationales pour la pratique professionnelle de l'audit interne*.

ANNEXE A : ÉVALUATION DES CRITÈRES D'AUDIT

Les attentes à l'égard de la DGIIT étaient les suivantes :	Note
Secteur d'intérêt A : Gouvernance	
A1 Élaborer un programme ou un cadre pour la continuité des activités de TI à l'appui de la gestion de la continuité des activités à l'échelle de l'organisation, en s'assurant notamment de ce qui suit :	
• L'énoncé de mission et les objectifs de l'équipe de planification de la continuité des activités de TI sont harmonisés avec les politiques du gouvernement du Canada et du ministère en matière de continuité des activités.	●
• Les rôles, les responsabilités et les obligations redditionnelles sont définis, adéquats et communiqués aux parties concernées, y compris aux intervenants et aux partenaires internes et externes.	◒
• Il existe, pour la planification de la continuité des activités de TI, des exigences et des mécanismes en matière de production de rapports qui sont adéquats et qui permettent une surveillance et une approbation opportunes des processus.	○
Secteur d'intérêt B : Gestion des risques	
B1 S'assurer que le cadre nécessite le recours à des évaluations des risques et à une analyse des répercussions sur les activités (ARA) pour la détermination des besoins essentiels en ressources, des stratégies de traitement de rechange et des approches en matière de reprise des activités.	◒
B2 S'assurer que les plans de continuité des activités de TI contiennent les résultats de l'évaluation des risques et des ARA en vue de l'établissement des expositions aux interruptions des activités, de la probabilité et des répercussions de ces interruptions ainsi que des solutions de rechange pour l'atténuation des risques.	◒
B3 Des OTR ont été établis pour fournir des lignes directrices concernant le temps requis pour le rétablissement ou fournir des services provisoires, et des OPR ont été établis pour fournir des lignes directrices au sujet de l'interruption ou de la perte maximale tolérable concernant les données.	◒
Secteur d'intérêt C : Gestion de programmes	
C1 Élaborer des plans dans le cadre du programme ou selon le cadre de planification de la continuité des activités de TI pour répondre aux exigences en matière de continuité des activités définies dans la PCA du ministère, en s'assurant notamment de ce qui suit :	
• Les applications et les plateformes de soutien essentielles ont été définies et les logiciels et les données nécessaires sont disponibles pour le traitement et la restauration provisoires et sont conformes à la PCA ministérielle.	◒
• Des procédures de récupération des données ont été établies pour assurer la disponibilité des données.	◒
• Les responsabilités du personnel ainsi que les procédures de notification, de substitution et d'accès sont en place pour permettre le rassemblement rapide du personnel et le lancement de procédures provisoires ou de restauration.	◒
• Le plan de reprise contient suffisamment de précisions pour permettre aux professionnels externes en matière de TI de le mettre en œuvre, si des membres du personnel ne sont pas disponibles.	◒
• Les fournisseurs tiers sont inclus dans les plans de continuité des activités de TI.	◒

• Les plans sont distribués selon le principe du besoin de savoir, ils sont conservés de manière sécuritaire et ils peuvent être obtenus à partir de plusieurs emplacements dans l'éventualité où le lieu de stockage principal serait compromis.	⊙
C2 Tenir à jour les plans de continuité des activités de TI de manière à ce qu'ils tiennent compte des modifications apportées à la PCA du ministère, en s'assurant notamment de ce qui suit :	
• Les plans sont maintenus selon un examen courant de leurs composantes, des résultats des essais et des liens avec les examens et les améliorations touchant la PCA du ministère.	○
• Les plans sont passés en revue dans le cadre des améliorations apportées aux applications et aux systèmes.	⊙
C3 Mettre à l'essai périodiquement les plans au moyen, entre autres, d'une vérification exhaustive des processus de continuité et d'exercices de mise en situation visant à vérifier les hypothèses et les procédures de rechange énoncées dans les plans.	⊙

✪ Pratiques exemplaires
● Contrôles suffisants ; exposition faible au risque
⊙ Contrôles suffisants, mais qui doivent être renforcés ; exposition moyenne au risque
○ Contrôles clés manquants ; exposition élevée au risque

ANNEXE B : GLOSSAIRE

ARA	Analyse des répercussions sur les activités
DGIIT	Direction générale de l'innovation, de l'information et de la technologie
DGSI	Direction générale des services d'intégrité
EDSC	Emploi et Développement social Canada
OPR	Objectif de point de rétablissement
OTR	Objectif de temps de reprise
PCA	Planification de la continuité des activités
SPC	Services partagés Canada
TI	Technologies de l'information