Vérification interne – Gestion des correctifs

Rapport final

Direction générale de la vérification, de l'évaluation et des risques

Agence du revenu du Canada | Canada Revenue Agency

Canada

© Sa Majesté le Roi du chef du Canada,
représentée par la Ministre du Revenu
national, 2026

No de catalogue Rv4-229/2026F-PDF

ISBN 978-0-662-72485-8

Le présent document est disponible sur le site Web du gouvernement du Canada à www.canada.ca

Le présent document est disponible en médias substituts sur demande.

Table des matières

Résumé exécutif **3**
Sommaire des recommandations 4
Réponse de la direction 4
Introduction **5**
Point de mire de la vérification interne **6**
Importance 6
Objectif 7
Portée 7
Critères et méthodologie de la vérification interne 7
Constatations, recommandations et plans d'action **7**
Observation 8
Surveillance et établissement de rapports 16
Remerciements **18**
Annexes **19**
Annexe A : Critères et méthodologie de la vérification interne 19
Annexe B : Glossaire 20

Résumé exécutif

Les pratiques de cybersécurité sont fondamentales pour la capacité de l'Agence du revenu du Canada (ARC) à remplir son mandat d'administration de l'impôt, des prestations et des programmes connexes, ainsi qu'à assurer l'observation pour le compte des gouvernements dans l'ensemble du Canada. Les lacunes dans les systèmes de cybersécurité et les retards dans la réponse aux vulnérabilités augmentent la probabilité que les cyberattaques réussissent, ce qui pourrait entraîner le vol de renseignements sensibles et nuire à la prestation des programmes et services aux Canadiennes et Canadiens.

Dans le cadre du dispositif de cybersécurité, la gestion des correctifs est l'une des nombreuses pratiques clés permettant de prévenir les compromissions, les atteintes à la sécurité des données, les perturbations opérationnelles et les événements défavorables. La gestion des correctifs est le processus de détermination, de priorisation, d'acquisition, d'installation et de vérification des correctifs (aussi appelés « travaux de réparation » ou « corrections » pour un élément de programmation), des mises à jour et des mises à niveau dans l'ensemble d'une organisation.

La gestion des correctifs est une responsabilité commune au sein de l'ARC, assumée en coordination avec les principaux organismes de sécurité du gouvernement du Canada. Au sein de l'ARC, la Direction générale de la sécurité (DGS) est responsable de la gestion des menaces de cybersécurité, des vulnérabilités liées à la cybersécurité et des événements de cybersécurité susceptibles de compromettre les réseaux et systèmes. La Direction générale de l'informatique (DGI) est responsable de l'acquisition, de la mise à l'essai, de la priorisation, du déploiement et de la vérification des correctifs à l'échelle de l'ARC, ainsi que de la supervision des calendriers des correctifs et du rendement lié au déploiement.

L'objectif de la vérification interne consistait à fournir au commissaire, à la direction de l'ARC et au Conseil de direction l'assurance que l'ARC corrige les vulnérabilités en matière de sécurité dans ses systèmes et ses applications de façon opportune et efficace.

Dans l'ensemble, l'équipe de la vérification interne a conclu que des instruments de politique d'entreprise sont en place et que les correctifs sont déployés pour traiter les vulnérabilités critiques et à risque élevé. [contenu caviardé]

L’équipe de la vérification interne a constaté ce qui suit :

- Les instruments de politique d’entreprise liés à la gestion des correctifs sont officiellement définis, à jour et communiqués.
  - [contenu caviardé]
  - [contenu caviardé]
  - [contenu caviardé]

Sommaire des recommandations

[contenu caviardé]

Réponse de la direction

La DGS et la DGI acceptent les recommandations formulées dans ce rapport et ont élaboré des plans d’action connexes. La Direction générale de la vérification, de l’évaluation et des risques a déterminé que les plans d’action sont adéquats pour donner suite aux recommandations.

Introduction

Les pratiques de cybersécurité sont fondamentales pour la capacité de l'Agence du revenu du Canada (ARC) à remplir son mandat, car les Canadiennes et Canadiens doivent faire confiance à l'ARC pour ce qui est de protéger leurs renseignements sensibles. Selon l'Évaluation des cybermenaces nationales 2025-2026[1], les cybermenaces, telles que les acteurs d'États-nations et les cybercriminels, recherchent continuellement des exploits et gagnent en sophistication grâce à l'intelligence artificielle. Les lacunes dans les systèmes de cybersécurité et les retards dans la réponse aux vulnérabilités augmentent la probabilité que les cyberattaques réussissent, ce qui pourrait entraîner le vol de renseignements sensibles et nuire à la prestation des programmes et services aux Canadiennes et Canadiens.

Dans le cadre du dispositif de cybersécurité, la gestion des correctifs est l'une des nombreuses pratiques clés permettant de prévenir les compromissions, les atteintes à la sécurité des données, les perturbations opérationnelles et les événements défavorables. La gestion des correctifs est le processus de détermination, de priorisation, d'acquisition, d'installation et de vérification des correctifs (aussi appelés « travaux de réparation » ou « corrections » pour un élément de programmation), des mises à jour et des mises à niveau dans l'ensemble d'une organisation[2].

La gestion des correctifs est une responsabilité commune au sein de l'ARC, assumée en coordination avec les principaux organismes de sécurité du gouvernement du Canada.

Au sein de l'ARC, le mandat de la Direction générale de la sécurité (DGS) consiste à permettre la prestation sans heurt des programmes et des services de l'ARC en assurant la protection du personnel, des renseignements et des biens de l'ARC. La DGS est responsable de la gestion des menaces de cybersécurité, des vulnérabilités liées à la cybersécurité et des événements de cybersécurité susceptibles de compromettre les réseaux et systèmes.

La Direction générale de l'informatique (DGI) élabore, exploite et maintient les technologies de l'information (TI) de l'ARC, et elle est responsable de l'acquisition, de la mise à l'essai, de la priorisation, du déploiement et de la vérification des correctifs à l'échelle de l'ARC, ainsi que de la supervision des calendriers de correctifs et du rendement lié au déploiement.

L'ARC coordonne également les activités liées à la sécurité avec les principaux organismes de sécurité du gouvernement du Canada et leurs partenaires. Le Secrétariat du Conseil du Trésor du Canada, le Centre de la sécurité des

---

[1] Évaluation des cybermenaces nationales 2025-2026 – Centre canadien pour la cybersécurité, https://www.cyber.gc.ca/fr/orientation/evaluation-cybermenaces-nationales-2025-2026

[2] NIST SP 800-40 Rev. 4, Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology, https://csrc.nist.gov/pubs/sp/800/40/r4/final

télécommunications Canada et le Centre canadien pour la cybersécurité assurent un leadership et fournissent des conseils et une orientation liés à la protection des infrastructures et des systèmes de TI gouvernementaux. Services partagés Canada est responsable de la planification, de la conception, de la construction, de l'exploitation et de la maintenance d'infrastructures et de services de TI efficaces, efficients et réactifs visant à sécuriser les réseaux et les systèmes de l'ARC[3].

Ces organisations travaillent ensemble pour prévenir le vol de données et limiter les perturbations des systèmes qui fournissent des programmes et services aux Canadiennes et Canadiens. Les directives du Secrétariat du Conseil du Trésor du Canada et du Centre canadien pour la cybersécurité accordent la priorité à l'application de correctifs aux systèmes d'exploitation et aux applications, qui constitue l'une des mesures de sécurité informatique les plus importantes, et elles fournissent des cadres de pratiques exemplaires pour soutenir les organisations gouvernementales[4,5].

Point de mire de la vérification interne

La présente vérification interne fait partie du Plan d'assurance et de consultation axé sur les risques de 2024-2025, qui a été approuvé par le Conseil de direction le 16 septembre 2024. Le cahier de planification a été approuvé par le commissaire le 18 juin 2025.

Importance

Un processus de gestion efficace des correctifs est un élément essentiel de la posture de cybersécurité d'une organisation, qui permet de s'assurer que les vulnérabilités sont rapidement traitées afin de réduire la possibilité d'exploitation.

Cette vérification interne fournit l'assurance que les principaux contrôles du processus de gestion des correctifs sont en place et fonctionnent comme prévu. La vérification interne appuie la haute direction de la DGS et de la DGI en fournissant des idées et des recommandations pour renforcer le processus de gestion des correctifs de ces directions générales.

---

[3] 2025 — Rapport de la vérificatrice générale du Canada au Parlement du Canada : La cybersécurité des réseaux et des systèmes du gouvernement, https://www.oag-bvg.gc.ca/internet/Francais/parl_oag_202510_04_f_44720.html

[4] 10 meilleures mesures de sécurité des TI, https://www.cyber.gc.ca/fr/orientation/10-meilleures-mesures-de-securite-des-ti-0

[5] Orientation sur la gestion des rustines, https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/securite-confidentialite-ligne/orientations-politiques-matiere-cybersecurite/orientation-gestion-rustines.html

Objectif

L'objectif de la vérification interne consistait à fournir au commissaire, à la direction de l'ARC et au Conseil de direction l'assurance que l'ARC corrige les vulnérabilités en matière de sécurité dans ses systèmes et ses applications de façon opportune et efficace.

Portée

La vérification interne a porté sur les systèmes de production essentiels, les applications, les appareils des points terminaux, les processus de soutien et les activités. La période visée par cette vérification interne s'est étendue du 1er janvier 2023 au 31 décembre 2024, mais les activités les plus récentes ont aussi été prises en considération lorsqu'elles étaient pertinentes.

La gestion des biens d'infrastructure, comme les ordinateurs centraux, les serveurs, les réseaux sous la gestion de Services partagés Canada et les services infonuagiques, ne faisait pas partie de la portée de cette vérification interne.

Critères et méthodologie de la vérification interne

Vous trouverez les critères et la méthodologie de la vérification interne à l'annexe A.

La phase d'examen de la vérification interne s'est déroulée de mai à septembre 2025.

La vérification interne a été menée conformément aux Normes internationales d'audit interne, comme le démontrent les résultats du programme de l'assurance de la qualité et d'amélioration.

Constatations, recommandations et plans d'action

Les recommandations formulées dans ce rapport visent à traiter les enjeux de grande importance ou les exigences obligatoires.

La DGS et la DGI acceptent les recommandations formulées dans ce rapport et ont élaboré des plans d'action connexes. La Direction générale de la vérification, de l'évaluation et des risques (DGVER) a déterminé que les plans d'action sont adéquats pour donner suite aux recommandations.

Observation

Les instruments de politique d'entreprise liés à la gestion des correctifs sont officiellement définis, à jour et communiqués.

Contexte

La vérification interne s'attendait à constater que les instruments de politique d'entreprise liés aux exigences de gestion des correctifs étaient documentés, à jour et publiés pour être communiqués aux intervenants.

Constatations

La vérification interne a révélé que les instruments de politique d'entreprise de l'ARC sont établis, à jour et approuvés. Les Normes à l'égard du renforcement des systèmes et de la gestion des correctifs de sécurité définissent des exigences pour les délais de déploiement des correctifs, la priorisation axée sur les risques et la gestion des exceptions et écarts. L'équipe de la vérification interne a noté que les changements apportés lors du quatrième trimestre de 2024-2025 aux exigences concernant les délais de déploiement des correctifs reflètent les récentes modifications apportées aux lignes directrices du Centre canadien pour la cybersécurité et du Secrétariat du Conseil du Trésor du Canada quant aux exigences en matière de correctifs d'urgence et à l'harmonisation des délais. Les normes sont publiées et accessibles sur des sites Web internes pour le personnel de l'ARC.

Pourquoi est-ce important?

Des politiques définies et claires pour assurer l'efficacité de la sécurité et de la gestion des correctifs renforcent la prise de décisions et permettent de veiller à ce que les intervenants s'harmonisent avec les objectifs organisationnels.

[contenu caviardé]

Contexte

La vérification interne s'attendait à ce qu'un processus soit en place pour :

- [contenu caviardé]
- [contenu caviardé]

[contenu caviardé]

Constatations

[contenu caviardé]

Pourquoi est-ce important?

[contenu caviardé]

Recommandation no 1

[contenu caviardé]

Réponse de la direction no 1 :

[contenu caviardé]

Réponse de la direction et plan d'action no 1a :

[contenu caviardé]

[contenu caviardé]

Réponse de la direction et plan d'action no 1b :

[contenu caviardé]

Réponse de la direction et plan d'action no 1c :

[contenu caviardé]

Réponse de la direction et plan d'action no 1d :

[contenu caviardé]

[contenu caviardé]

Contexte

La vérification interne s'attendait à constater que les correctifs avaient été :

- [contenu caviardé]
  [contenu caviardé]

- [contenu caviardé]

Constatations

[contenu caviardé]

[contenu caviardé]

[contenu caviardé]

Pourquoi est-ce important?

[contenu caviardé]

Recommandation no 2

[contenu caviardé]

Réponse de la direction et plan d'action no 2a :

[contenu caviardé]

[contenu caviardé]

Réponse de la direction et plan d'action no 2b et no 2c :

[contenu caviardé]

Réponse de la direction et plan d'action no 2d :

[contenu caviardé]

[contenu caviardé]

Réponse de la direction et plan d'action no 2e :

[contenu caviardé]

Surveillance et établissement de rapports

[contenu caviardé]

Contexte

La vérification interne s’attendait à constater que les indicateurs de rendement fournissent des renseignements précis et pertinents pour appuyer la prise de décisions liées au rendement de la gestion des correctifs au sein de l’ARC, et elle en a fait rapport à la haute direction.

Constatations

La vérification interne a révélé que des indicateurs de rendement étaient définis dans les tableaux de bord sur les rapports du Comité des cadres de la Direction générale de la DGI, et que les activités liées aux correctifs étaient surveillées. [contenu caviardé]

Pourquoi est-ce important?

[contenu caviardé]

Recommandation no 3

[contenu caviardé]

Réponse de la direction et plan d’action no 3

[contenu caviardé]

Remerciements

Pour conclure, la DGVER souhaite reconnaître et remercier la DGS et la DGI du temps accordé et des renseignements fournis dans le cadre de cette mission.

Annexes

Annexe A : Critères et méthodologie de la vérification interne

Critères de la vérification interne

Selon l'évaluation des risques de la DGVER, les secteurs d'intérêt suivants ont été cernés :

Secteurs d'intérêt	Critères
1. Observation	1.1 Les politiques, les directives, les normes et les procédures de l'ARC, y compris la gouvernance, liés à la gestion des correctifs, sont définies, à jour et communiquées aux intervenants.
	1.2 Les approches et les renseignements de gestion des risques sont utilisés pour évaluer et établir l'ordre de priorité des correctifs pour les systèmes et les applications.
	1.3 Les correctifs sont préparés et déployés conformément aux politiques et aux procédures.
2. Surveillance et établissement de rapports	2.1 Les indicateurs de rendement de la gestion des correctifs fournissent des renseignements exacts et pertinents pour appuyer la prise de décisions.

Méthodologie de la vérification interne

La méthodologie d'examen consistait à :

- examiner et analyser les instruments de politique d'entreprise et les documents à l'appui liés à la gestion des correctifs;
- mener des entrevues et des revues générales avec la direction et le personnel de la DGS et de la DGI;
- mettre à l'essai les contrôles, aux fins d'observation, par des examens des documents;
- examiner et analyser les données provenant d'applications et d'outils de soutien;
- examiner et analyser les indicateurs de rendement et les rapports de surveillance en place liés à la gestion des correctifs.

Annexe B : Glossaire

Terme	Définition
Application d'entreprise	Application développée par la DGI de l'ARC selon son processus de développement d'entreprise.
Atténuer	Terme défini pour mettre l'accent sur le fait que le concept d'atténuation des risques relatifs aux vulnérabilités de logiciel n'est pas la même chose que la correction. Quelle que soit la lacune, la défaillance ou la faute qui a mené à la détermination d'une vulnérabilité, le risque que l'ARC subisse un incident connexe est réduit par des mesures d'atténuation pendant que des plans sont élaborés et mis en œuvre pour résoudre le problème à la source.
Bibliothèque	Ensemble de dossiers, programmes, routines, scripts ou fonctions pouvant être mentionnés dans le code de programmation.
Bibliothèque non certifiée	Bibliothèque non enregistrée ou sans autre version certifiée dans le registre faisant autorité de tous les logiciels et composants réutilisables utilisés à l'ARC.
Contrôle	Moyen par lequel une organisation réduit la probabilité qu'un risque se concrétise ou limite l'incidence s'il se concrétise. Un contrôle devrait être un contrôle de prévention, de détection ou de correction, et doit être manuel ou automatisé (c'est-à-dire système).
Contrôle de sécurité	Exigence de sécurité générale en ce qui concerne la gestion, les opérations ou l'aspect technique, nécessaire à un système d'information afin de protéger la confidentialité, l'intégrité et la disponibilité de ses biens informatiques. Les contrôles de sécurité peuvent être appliqués à l'aide de diverses solutions de sécurité, dont des produits, politiques, pratiques et procédures de sécurité.

Correctif	« Travail de réparation » pour un élément de programmation; aussi appelé « correction ». Un correctif est la solution immédiate à un problème cerné qui est fournie aux utilisateurs; il peut parfois être téléchargé à partir du site Web du fabricant du logiciel.
Cyberattaque	Utilisation de moyens électroniques pour interrompre, manipuler ou détruire un système informatique, un réseau ou un appareil, ou pour obtenir un accès non autorisé à celui-ci.
Cybermenace	Acteur malveillant qui utilise Internet et tire avantage d'une vulnérabilité connue d'un produit pour exploiter un réseau et les renseignements qui y sont stockés.
Cybersécurité	Protection des renseignements numériques et préservation de l'intégrité de l'infrastructure qui abrite et transmet les renseignements numériques. Plus précisément, la cybersécurité englobe l'ensemble des technologies, processus, pratiques et mesures de réponse et d'atténuation conçus pour protéger les réseaux, les ordinateurs, les programmes et les renseignements contre les attaques, les dommages ou l'accès non autorisé afin d'assurer la confidentialité, l'intégrité et la disponibilité.
Évaluation des menaces et des risques	Processus qui consiste à déterminer quels sont les biens matériels dans une installation ou les biens informatiques dans un système, à évaluer comment ces biens peuvent être compromis, à évaluer le niveau de risque que représentent les menaces pour ces biens, et à recommander des mesures de sécurité pour atténuer les menaces.
Exploit	Outil logiciel, script ou code conçu pour tirer parti d'une ou de plusieurs vulnérabilités dans les logiciels, les micrologiciels ou le matériel qui pourraient compromettre les données ou les systèmes de l'ARC.
Point terminal	Périphérique physique qui se connecte à un réseau informatique et qui échange des renseignements avec ce réseau. Citons en exemple les appareils mobiles, les ordinateurs de bureau, les machines virtuelles, les appareils intégrés et les serveurs.

Posture de sécurité	Préparation globale d'une organisation à se défendre contre les cybermenaces, y compris les outils, les politiques, la formation et les plans d'intervention — tout ce qui contribue à la capacité d'une organisation à détecter et bloquer les attaques et à rebondir après celles-ci.
Vulnérabilité	Faille ou faiblesse dans la conception ou la mise en œuvre d'un système d'information ou de son environnement qui pourrait être exploitée pour nuire aux biens ou aux opérations d'une organisation.
Vulnérabilités et expositions courantes	Base de données sur les vulnérabilités en cybersécurité connues publiquement, qui fournit des identifiants uniques.