Agence du revenu du Canada | Canada Revenue Agency

VÉRIFICATION INTERNE – ÉVALUATION ET AUTORISATION DE LA SÉCURITÉ

Rapport final

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

Janvier 2023

Canada

No de catalogue Rv4-167/2023F-PDF

ISBN 978-0-660-46879-2

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

À mesure que les cybermenaces gagnent en sophistication et en ampleur, l'Agence du revenu du Canada (ARC) doit gérer un large éventail de risques pour la sécurité dans un environnement en évolution rapide. Une cyberattaque peut perturber la disponibilité des services numériques et menacer la sécurité des renseignements que les contribuables et les bénéficiaires de prestations ont soumis à l'ARC. L'**évaluation et l'autorisation de la sécurité** est un processus essentiel pour la fonction de sécurité de la technologie de l'information (TI) afin d'établir et de maintenir la confiance en la sécurité des systèmes d'information qui sont utilisés ou gérés par l'ARC, tout en tenant compte des besoins opérationnels en matière de sécurité.

Cette vérification interne portait sur le processus actuel d'évaluation et d'autorisation de la sécurité en place au sein de la Direction générale de la sécurité (DGS), qui est responsable de l'établissement de la gouvernance de la sécurité à l'ARC. La DGS est également responsable de la supervision des éléments de la TI et de la sécurité des données électroniques du programme de sécurité. En collaboration avec les intervenants du processus dans les directions générales, la DGS évalue le niveau de sécurité de tous les projets de TI et veille à ce que les risques résiduels liés à la sécurité de la TI relativement aux programmes, aux services et aux opérations soient évalués et approuvés de façon appropriée.

L'objectif de la vérification était de donner au commissaire, à la direction de l'ARC et au Conseil de direction l'assurance que les exigences en matière d'évaluation et d'autorisation de la sécurité sont en place et fonctionnent comme prévus.

Globalement, l'équipe de la vérification interne a constaté que le processus d'évaluation et d'autorisation de la sécurité ainsi que les exigences relatives aux systèmes de renseignements étaient appliqués dans les évaluations de la sécurité. Toutefois, elle a constaté que des améliorations sont nécessaires pour renforcer davantage les instruments de politique d'entreprise, les rôles et les responsabilités, l'autorisation, la surveillance des indicateurs de rendement et l'élaboration de procédures et d'outils officiels afin de répondre aux besoins de l'ARC.

Sommaire des recommandations

- La DGS devrait s'assurer que les instruments de politique d'entreprise soient examinés, actualisés et communiqués pour refléter la création de la DGS et qu'ils sont alignés sur les politiques actuelles du gouvernement du Canada.
- La DGS devrait élaborer des procédures, des lignes directrices, des normes, des outils et une sensibilisation dans le cadre de son processus d'évaluation et d'autorisation de la sécurité pour :
    - aider les intervenants dans le processus visant à produire efficacement des documents justificatifs complets à l'appui de l'évaluation et de l'autorisation de la sécurité pour les évaluations et les activités de gestion des risques;
    - intégrer les lignes directrices du gouvernement du Canada sur les activités de gestion des risques liés à la sécurité infonuagique dans les procédures d'évaluation et de surveillance;

    - veiller à ce que les exigences soient en place pour mettre en œuvre des outils permettant de gérer efficacement le processus d'évaluation et d'autorisation de la sécurité.
- La DGS, en consultation avec la Direction générale de l'informatique (DGI), devrait veiller à ce que les rôles, les responsabilités et les critères d'évaluation et d'autorisation de la sécurité soient communiqués et compris par les intervenants dans le processus et intégrés tôt dans la planification des projets de TI sans points de contrôle et des systèmes grandement modifiés. Ainsi, la DGS devrait envisager d'officialiser l'intégration de l'évaluation et de l'autorisation de la sécurité dans le processus de gestion des ordres de travail de la TI.
- La DGS devrait actualiser ses processus et ses procédures actuels afin de s'assurer qu'une autorisation a été obtenue et consignée pour toutes les applications, tous les systèmes et toutes les composantes avant de passer à la production.
- La DGS devrait élaborer une stratégie de surveillance centralisée des autorisations des systèmes pour toute l'ARC afin de conserver les autorisations et de consigner les décisions en matière de sécurité fondées sur les risques.
- La DGS, en consultation avec la DGI et les intervenants, devrait s'assurer que les inventaires, les outils et les documents justificatifs sont exacts et complets afin de prioriser l'examen des applications, des systèmes et des composantes pour obtenir les autorisations d'exploitation.
- La DGS devrait élaborer des mécanismes de surveillance pour assurer l'achèvement en temps voulu des plans de mise en œuvre des mesures de protection, la production de rapports sur la conformité au processus d'évaluation et d'autorisation de la sécurité, et l'efficacité continue des contrôles de sécurité.

Réponse de la direction

La DGS accepte les recommandations formulées dans ce rapport et a dressé 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.

1. Introduction

L'Agence du revenu du Canada (ARC) contribue au mieux-être économique et social des Canadiens et à l'efficience du gouvernement en assurant une administration de l'impôt et des prestations de calibre mondial qui est réceptive, efficace et fiable[1]. L'une des priorités de l'ARC est d'améliorer l'expérience de service centrée sur le client en transformant les services numériques qu'elle offre aux Canadiens tout en gagnant et en maintenant la confiance du public. Alors que les Canadiens utilisent et comptent de plus en plus sur les services numériques, l'ARC possède l'un des plus importants environnements de TI et dépôts de renseignements personnels et financiers du gouvernement du Canada. Au cours de l'exercice de 2020 à 2021, 90,2 % des déclarations de revenus et de prestations, et 94,2 % des déclarations de revenus des entreprises ont été produites par voie électronique[2].

La sécurité de la TI exige une gouvernance à l'échelle de l'organisation ainsi qu'un effort et une diligence soutenus pour assurer la mise en œuvre de mesures de protection afin de préserver la confidentialité, l'intégrité, la disponibilité, l'utilisation prévue et la valeur des renseignements stockés, traités ou transmis par voie électronique. Une approche efficace des contrôles de sécurité axée sur la gestion des risques doit être établie, surveillée, maintenue et révisée, et des mesures correctives doivent être prises rapidement lorsque des problèmes sont décelés.

Au fur et à mesure que les cybermenaces gagnent en sophistication et en ampleur, l'ARC, en partenariat avec Services partagés Canada et les principales agences de sécurité, doit s'assurer de gérer un large éventail de risques pour la sécurité dans un environnement qui évolue rapidement. Une cyberattaque peut perturber la disponibilité des services numériques et menacer la sécurité des renseignements que les contribuables et les bénéficiaires de prestations ont soumis à l'ARC. Il est essentiel que l'ARC réponde aux attentes des Canadiens à l'égard de la prestation de services à la clientèle tout en leur assurant que leurs renseignements seront à l'abri des atteintes potentielles à la protection des données et du vol d'identité.

L'évaluation et l'autorisation de la sécurité est un processus essentiel pour le programme de sécurité de la TI afin d'établir et de maintenir la confiance envers la sécurité des systèmes d'information qui sont utilisés ou gérés par l'ARC, tout en tenant compte des besoins opérationnels en matière de sécurité. L'évaluation de la sécurité est le processus continu d'évaluation des pratiques et des contrôles de sécurité visant à déterminer s'ils sont mis en œuvre correctement, fonctionnent comme prévu et produisent les résultats souhaités en ce qui concerne le respect des exigences de sécurité définies. L'autorisation de sécurité est le processus continu visant à obtenir et à maintenir une décision sur la gestion des risques pour la sécurité et à accepter explicitement le risque résiduel avec l'autorisation d'exploitation, en fonction des résultats de l'évaluation de la sécurité. Ce processus se déroule parallèlement avec le cycle de développement des systèmes de l'ARC, afin de faciliter la conception de systèmes sécurisés pour la protection des renseignements et des services. En 2013, l'ARC a approuvé sa directive initiale sur l'évaluation et l'autorisation de la sécurité, en conformité avec le cadre stratégique du programme de sécurité de l'ARC, la politique sur la sécurité et la directive sur la sécurité des renseignements et des systèmes.

[1] Mission, vision, promesse et valeurs de l'ARC – Canada.ca
[2] Rapport sur les résultats ministériels 2020-2021 de l'ARC – Canada.ca

Au cours de l'exercice de 2021 à 2022, l'ARC a créé la DGS, regroupant les programmes de sécurité fonctionnels afin d'établir une approche coordonnée pour continuer à protéger ses employés, ses renseignements et ses biens, et de faire en sorte que les risques liés à la sécurité soient gérés de façon proactive et continue. La sécurité de la TI et l'évaluation et l'autorisation de la sécurité sont des responsabilités partagées au sein de l'ARC, comme il est détaillé ci-dessous.

Sous-commissaire de la DGS et agent de sécurité de l'ARC

- Est responsable de la gestion et de l'orientation du programme de sécurité
- Veille à ce que le cadre de gouvernance et l'infrastructure appropriés soient établis

Directeur général de la Direction de la cybersécurité et de la sécurité de l'information de la DGS et dirigeant principal de la sécurité de l'information

- Est responsable de la supervision des éléments de la sécurité de la TI et des données électroniques du programme de sécurité
- Agit à titre de responsable fonctionel des processus d'évaluation et d'autorisation de la sécurité.
- Évalue la posture de sécurité de tous les projets de TI et veille à ce que les risques résiduels liés à la sécurité de la TI associés aux programmes, aux services et aux opérations soient évalués et approuvés de façon appropriée pour l'exploitation

Division de la cybersécurité de la Direction de la cybersécurité et de la sécurité de l'information de la DGS

- Administre le programme d'évaluation et d'autorisation de la sécurité, fournit un soutien et une orientation sur toutes les exigences en matière de sécurité, évalue le niveau de risque global, et surveille et communique l'état des plans de mise en œuvre des mesures de protection

Responsables opérationnels au sein des directions générales

- S'assurent que toutes les applications et tous les systèmes font l'objet d'une évaluation de la sécurité et sont conçus, élaborés, intégrés, mis à l'essai et installés conformément aux exigences en matière de sécurité de la TI
- Acceptent officiellement tous les risques résiduels pour la sécurité de la TI associés aux programmes, aux services et aux activités dont ils sont responsables

Gestionnaires de projets et exécuteurs de systèmes

- Aident les responsables opérationnels à assurer le respect des exigences en matière de sécurité des projets
- Intègrent le processus d'évaluation et d'autorisation de la sécurité et les produits livrables dans le plan de projet global et le cycle de développement des systèmes

Alors que l'ARC continue d'examiner la prestation de nouveaux services numériques et les technologies émergentes, il est essentiel que la sécurité de la TI soit intégrée dès les premières étapes des nouveaux programmes et initiatives, et à la conception de systèmes d'information sécurisés et fiables.

2. Point de mire de la vérification

La présente vérification interne fait partie du plus récent Plan d'assurance et de consultation axé sur les risques de 2021-2022 qui a été approuvé par le Conseil de direction. Le cahier de planification a été approuvé par le commissaire le 26 janvier 2022.

2.1. Importance

Les atteintes à la vie privée et les cyberattaques menaçant les données et les biens de nature délicate peuvent avoir de graves conséquences pour les organisations, allant des pertes financières aux préjudices réputationnels. L'évaluation et l'autorisation de la sécurité constituent une pratique essentielle qui garantit que la sécurité est intégrée dès les premières étapes des nouveaux programmes, et que les risques pour la sécurité des systèmes, des composantes et des applications de l'ARC sont décelés et gérés de façon appropriée. Cette vérification est liée aux risques d'entreprise cernés dans le profil des risques de l'entreprise de l'ARC sur la protection des renseignements des contribuables et la cybersécurité.

2.2. Objectif

L'objectif de la vérification consistait à fournir au commissaire, à la direction de l'ARC et au Conseil de direction l'assurance que les exigences en matière d'évaluation et d'autorisation de la sécurité étaient en place et fonctionnaient comme prévus.

2.3. Portée

La vérification a porté sur les systèmes de production, les composantes, les applications, les processus de soutien et les activités de l'ARC en date du 31 décembre 2021.

L'équipe de vérification a mené des entrevues à l'Administration centrale avec la DGS, la DGI, la Direction générale de cotisation, de prestation et de service, la Direction générale des appels, la Direction générale des recouvrements et de la vérification et la Direction générale des programmes d'observation.

Les biens d'infrastructure, comme les ordinateurs centraux, les serveurs, le réseau et l'infrastructure en nuage gérés par Services partagés Canada, étaient exclus de la vérification.

2.4. Critères et méthodologie de la vérification

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

La phase d'examen de la vérification s'est déroulée entre décembre 2021 et mai 2022.

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

3. Constatations, recommandations et plans d'action

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

3.1. Observation

3.1.1 Des instruments de politique d'entreprise existent et sont communiqués. Toutefois, étant donné la récente réorganisation de la Direction générale des finances et de l'administration et la création de la DGS, ils ne sont ni à jour ni harmonisés avec les politiques du gouvernement du Canada.

La DGS a examiné, publié et communiqué les instruments de politique de sécurité d'entreprise concernant l'évaluation et l'autorisation de la sécurité.

Au moment de l'examen, les instruments de politique d'entreprise n'étaient pas à jour en raison de la création de la DGS et n'étaient pas non plus harmonisés avec les politiques actuelles du gouvernement du Canada. Plus particulièrement, ils ne reflétaient pas les responsabilités élargies du nouvel agent de sécurité de l'ARC et faisaient référence à des politiques désuètes du gouvernement du Canada. De plus, la Directive sur l'évaluation et l'autorisation de la sécurité n'a pas été actualisée pour prendre la DGS en compte en tant que propriétaire opérationnel. Cette situation pourrait entraîner des règles de gouvernance et des responsabilités insuffisamment claires pour assurer la bonne gestion des risques liée à la sécurité de la TI relatifs aux programmes, aux services et aux opérations de l'ARC ainsi qu'à la protection des personnes, des renseignements et des biens. L'équipe de la vérification interne a examiné les plans d'ébauche des instruments de politique d'entreprise devant être mis à jour par la DGS, qui n'était pas en place au moment où la vérification a été réalisée.

Recommandation 1

La DGS devrait s'assurer que les instruments de politique d'entreprise soient examinés, actualisés et communiqués pour refléter la création de la DGS et qu'ils sont alignés sur les politiques actuelles du gouvernement du Canada.

Plan d'action 1

La DGS travaillera avec les intervenants pour mettre à jour la Directive sur l'évaluation et l'autorisation de la sécurité, d'abord pour tenir compte de sa propre création, et aussi pour s'assurer que ces instruments sont en harmonie avec les politiques actuelles du gouvernement du Canada.

La date d'achèvement cible pour ce plan d'action est octobre 2023.

3.1.2 Les rôles et les responsabilités des intervenants sont définis et communiqués. Toutefois, il est possible de s'assurer qu'elles sont comprises par tous les intervenants impliqués dans le processus d'évaluation et d'autorisation de la sécurité.

Les rôles et les responsabilités concernant la gestion de l'évaluation et de l'autorisation de la sécurité au sein de l'ARC sont clairement définis et publiés dans les instruments de politique d'entreprise.

Toutefois, l'équipe de vérification interne a vu des occasions pour s'assurer que les rôles et responsabilités soient bien compris. Les entrevues avec les intervenants ont révélé qu'ils

n'étaient pas toujours au courant du processus d'évaluation et d'autorisation de la sécurité, ou qu'ils ne le comprenaient pas bien, plus précisément en ce qui concerne la surveillance, et en particulier les intervenants qui n'ont pas récemment participé à la réalisation d'une évaluation et d'une autorisation de la sécurité ou qui étaient nouveaux dans leur rôle respectif. Un certain nombre de facteurs ont été indiqués comme causes du manque de compréhension des intervenants inexpérimentés, dont le roulement dans les rôles clés des intervenants, le manque de formation sur l'évaluation et l'autorisation de la sécurité, ainsi qu'une communication et une sensibilisation limitées auprès des intervenants. Cette situation pourrait entraîner une observation incohérente des exigences législatives et politiques, et la perte potentielle de renseignements protégés et classifiés.

Voir les recommandations 1 et 3.

3.1.3 Des évaluations de la sécurité des systèmes d'information sont effectuées. Toutefois, il existe des possibilités d'améliorer les procédures officielles, les lignes directrices, les normes, la sensibilisation et les outils pour gérer efficacement le processus d'évaluation et d'autorisation de la sécurité.

Les évaluations de la sécurité garantissent que les systèmes sont conçus, développés, configurés et installés avec une posture de sécurité appropriée et constituent le fondement de la confiance des divers utilisateurs envers les systèmes de l'ARC, à savoir le personnel, les clients, les partenaires et les contribuables. Les instruments de politique d'entreprise de l'ARC indiquent que la DGS doit documenter un processus d'évaluation et d'autorisation de la sécurité qui fournit une assurance de sécurité adéquate des systèmes et les logiciels de l'ARC pour prendre des décisions éclairées concernant les autorisations.

L'équipe de vérification interne a constaté qu'un processus général d'évaluation et d'autorisation de la sécurité était documenté et disponible. L'information sur le processus d'évaluation et d'autorisation de la sécurité a été consignée à divers endroits, notamment sur les pages intranet et wiki internes de l'ARC, dans les diagrammes de flux de travail et dans divers modèles. Selon un échantillon de 10 évaluations de la sécurité effectuées au cours de l'exercice de 2020-2021, il existait généralement des documents, remplis par un évaluateur de la sécurité, pour étayer les rapports d'évaluation de la sécurité. Les rapports d'évaluation de la sécurité comprenaient les risques décelés et des recommandations pour corriger les lacunes. Ces rapports ont été dûment approuvés par le directeur de la Division de la cybersécurité de la DGS. Au moment de l'examen, la DGS révisait le processus d'évaluation et d'autorisation de la sécurité dans le cadre d'un exercice d'amélioration des processus et d'une initiative visant à étudier et à mettre en œuvre une solution disponible sur le marché pour appuyer les processus de sécurité.

L'équipe de vérification interne a déterminé que le processus d'évaluation et d'autorisation de la sécurité ne comportait pas de procédures et de lignes directrices officielles et centralisées. Cette lacune pourrait être corrigée afin d'assurer l'exhaustivité et l'approbation éclairée des documents justificatifs et des analyses de la vulnérabilité, de la création de modèles uniformes pour l'évaluation et le calcul des risques, et de l'intégration des lignes directrices du gouvernement du Canada sur les activités de gestion des risques liés à la sécurité infonuagique dans les procédures d'évaluation et de surveillance.

L'équipe de vérification interne a également déterminé qu'il existe des outils en place, par exemple PROTÉGÉ et les feuilles de calcul utilisées pour produire des rapports. Toutefois, ces solutions conçues localement ne répondent pas aux

besoins en matière de suivi, de surveillance des risques et de production de rapports du processus d'évaluation et d'autorisation de la sécurité.

De plus, ce que les intervenants connaissent du processus d'évaluation et d'autorisation de la sécurité dépend de leur expérience antérieure. De plus, les nouveaux intervenants et gestionnaires de projets ont de la difficulté à comprendre le processus en raison d'un manque de formation. Il est essentiel d'aborder les questions de sécurité dès les premières étapes des projets de TI et tout au long du cycle de vie des systèmes d'information pour s'assurer que la sécurité est intégrée à la conception, que les objectifs de sécurité sont atteints et, que la planification et les ressources sont optimisées. Bien que le processus d'évaluation et d'autorisation de la sécurité ait été intégré au processus de gestion de projet, plus précisément au cadre d'évaluation des points de contrôle des projets de la DGI pour les grands projets de TI, les petits projets de TI et les améliorations des systèmes ne sont pas toujours tenus de suivre le cadre. De plus, les intervenants ne comprenaient pas bien les lignes directrices et les éléments déclencheurs permettant d'engager de manière proactive la DGS au début du processus de planification, ainsi que la définition d'un changement important parmi les critères de réévaluation. Par conséquent, les petits projets de TI et les améliorations des systèmes n'ont pas toujours été intégrés dès les premières étapes parmi les facteurs à considérer dans l'évaluation et l'autorisation de la sécurité, ce qui pourrait causer un manque de fiabilité dans les opérations des services, des retards dans la mise en œuvre de nouveaux services, une affectation insuffisante de ressources et des vulnérabilités en matière de sécurité laissées sans prise en compte adéquate des risques pour la sécurité.

Recommandation 2

La DGS devrait élaborer des procédures, des lignes directrices, des normes, des outils et des campagnes de sensibilisation dans le cadre de son processus d'évaluation et d'autorisation de la sécurité pour :

- **aider les intervenants dans le processus à produire efficacement des documents justificatifs complets à l'appui de l'évaluation et de l'autorisation de la sécurité pour les évaluations et les activités de gestion des risques;**
- **intégrer les lignes directrices du gouvernement du Canada sur les activités de gestion des risques liés à la sécurité infonuagique dans les procédures d'évaluation et de surveillance;**
- **veiller à ce que des exigences soient appliquées à la mise en œuvre d'outils pour gérer efficacement le processus d'évaluation et d'autorisation de la sécurité.**

Plan d'action 2

Au début de 2022, la DGS a entrepris un examen de ses flux de travail et de ses processus internes afin de déterminer les éléments à améliorer. L'objectif de l'amélioration de l'évaluation et de l'autorisation de la sécurité consistait à accroître l'uniformité, la réutilisabilité et la répétabilité du processus. De plus, des efforts importants ont été déployés pour augmenter l'efficacité et la souplesse dans le but d'améliorer la qualité de l'évaluation et de permettre à l'organisation de perfectionner l'intégration de la cybersécurité dès les premières étapes du développement (conception intégrée de la sécurité). La DGS concevra un processus d'évaluation et d'autorisation de la sécurité uniforme et officialisé, des procédures détaillées, des lignes directrices, des outils et du matériel d'information pour les flux de travail internes associés à ce processus. De plus, elle aidera les intervenants à gérer efficacement les documents à l'appui de l'évaluation et de

l'autorisation de la sécurité pour les évaluations et les activités de gestion des risques et intégrera les lignes directrices du gouvernement du Canada sur les activités de gestion des risques liés à la sécurité infonuagique dans les procédures d'évaluation et de surveillance.

La DGS veillera à ce que des exigences soient appliquées à la mise en œuvre continue d'outils de soutien pour gérer efficacement le processus d'évaluation et d'autorisation de la sécurité.

La date d'achèvement cible pour ce plan d'action est décembre 2023.

Recommandation 3

La DGS, en consultation avec la DGI, devrait veiller à ce que les rôles, les responsabilités et les critères d'évaluation et d'autorisation de la sécurité soient communiqués et compris par les intervenants dans le processus et intégrés tôt dans la planification des projets de TI sans points de contrôle et des systèmes grandement modifiés. De plus, elle devrait envisager d'officialiser l'intégration de l'évaluation et de l'autorisation de la sécurité dans le processus de gestion des ordres de travail de la TI.

Plan d'action 3

La DGS travaillera avec les intervenants pour mettre à jour la Directive sur l'évaluation et l'autorisation de la sécurité afin de tenir compte des changements apportés aux rôles et aux responsabilités à la suite de la création de la DGS. Durant ce processus, les intervenants sont consultés pour obtenir des renseignements et de la rétroaction sur les changements. Une fois que les mises à jour seront terminées et approuvées, la DGS travaillera avec les équipes appropriées pour publier un article dans les Nouvelles de l'Agence sur InfoZone afin de communiquer les changements.

La date d'achèvement cible pour ce plan d'action est mars 2023.

Le projet d'amélioration de l'évaluation et de l'autorisation de la sécurité a marqué un tournant, où les améliorations continues, l'autoévaluation et les ajustements sont devenus la norme. Dans le cadre de cette initiative, le processus d'évaluation initial de l'évaluation et de l'autorisation de la sécurité a été examiné, une méthode d'évaluation et d'autorisation de la sécurité par niveau a été introduite, les flux de travail ont été examinés, et les modèles d'évaluation et d'autorisation de la sécurité utilisés pour les activités quotidiennes ont été simplifiés et actualisés.

Des modèles de sécurité ont été créés pour adopter une approche de « conception intégrée » plutôt que réactive à l'évaluation de la sécurité. Au fur et à mesure que les changements seront mis en œuvre, on s'attend à ce que des améliorations soient progressivement apportées aux projets d'évaluation et d'autorisation de la sécurité en cours.

Comme le nombre de demandes d'évaluation et d'autorisation de la sécurité augmente de façon exponentielle, la DGS élargira son rôle dans la coordination en exploitant son processus d'évaluation initial afin de s'assurer que ses produits livrables de sécurité sont achevés aux dates cibles. Cette mesure permettra de s'assurer que les intervenants comprennent bien les rôles et les responsabilités dans l'évaluation et l'autorisation de sécurité dans les projets avec ou sans points de contrôle et fera mieux connaître à la DGI les améliorations apportées au processus. De plus, elle aidera à amorcer une discussion sur une meilleure intégration des composantes du processus d'évaluation et d'autorisation de la sécurité dans la gestion des ordres de travail de la TI.

La date d'achèvement cible pour ce plan d'action est décembre 2023.

3.1.4 Les autorisations d'exploitation des systèmes d'information dans l'environnement de production ne sont pas toujours à jour, documentées, dûment approuvées et maintenue continuellement tout au long du cycle de vie opérationnel.

L'autorisation (autorisation d'exploitation) est une étape continue essentielle dans le processus d'évaluation et d'autorisation de la sécurité. Il s'agit de la décision officielle et de l'acceptation formelle des risques consignés dans le rapport d'évaluation de la sécurité par une autorité désignée pour approuver un système d'information aux fins d'utilisation opérationnelle dans l'environnement de production tout au long du cycle de vie opérationnel.

L'équipe de la vérification interne a constaté que l'autorisation d'exploitation des systèmes d'information en production n'était pas toujours à jour, documentée ou dûment approuvée. Lors d'un examen de 10 évaluations de sécurité effectuées au cours de l'année 2020-2021, l'équipe de la vérification interne a trouvé cinq cas où l'autorisation n'a pas été maintenu correctement ou n'a pas été approuvée par les responsables opérationnels comme l'exige la politique. L'équipe de vérification interne a également noté un cas où l'autorisation n'a pas été signée avant les dates de production comme l'exige la politique de l'ARC.

L'équipe de la vérification interne a également examiné les applications de production d'entreprise existantes et n'a pas été en mesure de déterminer si un processus d'évaluation et d'autorisation de la sécurité existait ou avait été maintenu pour l'ensemble des applications, des systèmes, des composantes et de l'infrastructure de soutien. Plus précisément, l'équipe a constaté des problèmes de gestion de l'information et d'intégrité des données concernant les outils dans le répertoire des applications des solutions, PROTÉGÉ , et les feuilles de calcul des examens périodiques. L'équipe de la vérification interne a également constaté que ce ne sont pas toutes les applications d'entreprise qui peuvent être facilement rattachées à une autorisation d'exploitation signée ou à une évaluation plus ancienne des menaces et des risques en raison d'un manque de surveillance de la gestion et parce qu'il n'y a pas de répertoire centralisé dûment géré. Certains secteurs opérationnels et secteurs de soutien n'avaient pas connaissance de documents justificatifs pour les évaluations ou les autorisations de sécurité actuelles, ou n'avaient pas conservé ces documents.

De plus, l'équipe de vérification interne a noté que la DGS documente l'étape générale de la surveillance continue et la nécessité de maintenir l'autorisation à mesure que les menaces et les risques pour les systèmes d'information et l'environnement opérationnel continuent d'évoluer au fil du temps. L'équipe de vérification a aussi constaté l'absence de procédures de surveillance officielles pour les intervenants. Également, ce ne sont pas tous les intervenants qui effectuent une surveillance constante pour conserver l'autorisation tout au long du cycle de vie opérationnel du système d'information. D'après l'examen du sondage sur la gestion du portefeuille des applications réalisé en 2021, un certain nombre de répondants n'avaient pas régulièrement examiné ou n'étaient pas au courant de la pertinence de l'évaluation et l'autorisation de la sécurité ou des évaluations des menaces et des risques plus anciennes pour répondre aux besoins opérationnels.

En menant des entrevues, l'équipe de la vérification interne a noté que diverses activités de sécurité de la TI ont été effectuées, notamment dans plusieurs domaines d'application où des mises à jour ont été apportées à l'évaluation de la sécurité relativement aux

lancements et aux grands projets de TI, aux activités locales spécifiques ou aux contrôles particuliers qui comprenaient la gestion des risques et des vulnérabilités en matière de sécurité. Toutefois, ces activités n'ont pas été consignées ou déclarées selon une approche uniforme et officielle de l'évaluation et de l'autorisation de la sécurité. L'équipe de vérification interne a noté que certains domaines d'application n'étaient pas toujours consultés par la DGS ou au courant des exigences spécifiques de surveillance et a noté le manque de directives et de capacité à rendre compte et documenter de façon centralisée les résultats de l'examen effectué afin de conserver l'autorisation tout au long du cycle de vie opérationnel du système d'information.

L'absence d'un processus approprié pour obtenir et conserver une autorisation pourrait entraîner des évaluations de la sécurité désuètes et que les changements et les risques ne soient pas gérés de façon proactive, ce qui pourrait entraîner de nouvelles vulnérabilités en matière de sécurité et une interruption des services essentiels pour les contribuables.

Recommandation 4

La DGS devrait actualiser ses processus et ses procédures actuels afin de s'assurer qu'une autorisation a été obtenue et consignée pour toutes les applications, tous les systèmes et toutes les composantes avant de passer à la production.

Plan d'action 4

Au début de l'année 2022, la DGS a entrepris un examen de ses flux de travail et de ses processus internes afin de déterminer quels éléments améliorer. Dans le cadre de cette initiative, l'autorisation d'exploiter le suivi, les processus et les risques résiduels associés pour l'organisation a été examinée.

Bien que la DGS puisse seulement s'assurer qu'une autorisation d'exploitation soit accordée après une évaluation de la sécurité des systèmes, certaines lacunes ont été relevées au cours du processus initial relativement aux modèles utilisés et aux processus d'autorisation d'exploitation. Par conséquent, la DGS a déterminé que la sensibilisation à l'évaluation et l'autorisation de la sécurité était insuffisante et qu'il n'y avait pas assez de produits livrables associés à l'évaluation et à l'autorisation de la sécurité à même la planification des projets. Par conséquent, il se peut que le système soit mis en production sans autorisation officielle parce qu'il n'est pas passé par le processus d'évaluation et d'autorisation de la sécurité initial. Des changements ont été opérés en juin 2022. D'autres mesures seront prises en ce qui concerne la sensibilisation au processus d'évaluation et d'autorisation de la sécurité et les intégrations de projets. Cette sensibilisation sera sous forme de formations offertes dans toutes les directions générales et de documents de sensibilisation qui seront disponibles sur les pages InfoZone et Wiki ou dans d'autres publications internes. De plus, des démarches seront entreprises en collaboration avec la DGI pour déterminer quelles applications et quels systèmes en exploitation n'ont pas d'évaluation de la sécurité valide.

La DGS doit approuver et mettre en œuvre le Conseil des risques en matière de cybersécurité.

La date d'achèvement cible pour ce plan d'action est mars 2023.

Recommandation 5

La DGS devrait élaborer une stratégie de surveillance centralisée des autorisations des systèmes pour l'ensemble de l'ARC afin de conserver les autorisations et de consigner les décisions en matière de sécurité axées sur les risques.

Plan d'action 5

Au début de 2022, la DGS a entrepris un examen de ses flux de travail et de ses processus internes afin de déterminer quels éléments améliorer. Dans le cadre de cette initiative, l'autorisation d'exploiter le suivi, les processus et les risques résiduels associés pour l'organisation a été examinés.

Bien que la DGS puisse seulement s'assurer qu'une autorisation d'exploitation soit accordée après une évaluation des systèmes, certaines lacunes en lien avec les modèles utilisés et les processus d'autorisation d'exploitation ont été relevées au cours du processus initial. Par conséquent, la DGS a déterminé que la sensibilisation à l'évaluation et l'autorisation de la sécurité était insuffisante et qu'il n'y avait pas assez de produits livrables associés à l'évaluation et à l'autorisation de la sécurité à même la planification des projets. Par conséquent, il se peut que le système soit mis en production sans autorisation officielle parce qu'il n'est pas passé par le processus initial d'évaluation et d'autorisation de la sécurité. Des changements ont été opérés en juin 2022.

Afin d'avoir une vue d'ensemble des autorisations des systèmes, l'ARC aura besoin d'une stratégie de surveillance centralisée des autorisations des systèmes à l'échelle de l'ARC qui nécessitera l'utilisation de plusieurs sources de renseignements de la DGI et de la DGS pour fournir un portrait réel de l'état des autorisations des systèmes au sein de l'organisation.

Au départ, des discussions avec la DGI seront nécessaires pour intégrer leurs flux de travail aux processus de la DGS afin de s'assurer que les aperçus de tous les systèmes en production, ou en cours d'élaboration, sont disponibles.

Deuxièmement, la DGS aura besoin d'un bon outil d'entreprise pour appuyer l'intégration des données (p. ex. un outil de gouvernance, de risque et d'observation), afin d'être en mesure de suivre, examiner et déterminer les systèmes n'ont pas d'autorisation appropriée ou qui nécessite un examen.

Ces données seront ensuite acheminées au Conseil des risques en matière de cybersécurité tous les trimestres aux fins d'information et de prise de décisions.

La DGS doit approuver et mettre en œuvre le Conseil des risques en matière de cybersécurité.

La date d'achèvement cible pour ce plan d'action global est mars 2024, tandis que certaines composantes seront achevées d'ici mars 2023.

Recommandation nº 6

La DGS, en consultation avec la DGI et les intervenants, devrait s'assurer que les inventaires, les outils et les documents justificatifs soient exacts et complets afin de prioriser l'examen des applications, des systèmes et des composantes pour obtenir les autorisations d'exploitation.

Plan d'action 6

Bien que la DGS puisse seulement s'assurer qu'une autorisation d'exploitation soit accordée après une évaluation des systèmes, certaines lacunes en lien avec les modèles utilisés et les processus d'autorisation d'exploitation ont été relevées au cours du processus d'évaluation initial. Par conséquent, la DGS a déterminé que la sensibilisation à l'évaluation et l'autorisation de la sécurité était insuffisante et que l'intégration des produits livrables de l'évaluation et l'autorisation de la sécurité dans la planification des projets étaient insuffisante. Par conséquent, il se peut qu'un système ait été mis en production sans autorisation officielle parce qu'il n'est pas passé par le processus initial d'évaluation et d'autorisation de la sécurité. Des changements ont été mis en place en juin 2022. D'autres mesures seront prises en ce qui concerne la sensibilisation au processus d'évaluation et d'autorisation de la sécurité et mieux intégrer les projets.

La DGS continuera de travailler avec la DGI afin d'améliorer les données disponibles, ce qui permettra d'établir un inventaire exact des systèmes qui sont en exploitation et le statut de leur autorisation.

Jusqu'à ce que l'ARC mette en place une stratégie de surveillance centralisée des autorisations des systèmes dans l'ensemble de l'organisation et qu'un inventaire ou une représentation exacte des autorisations des systèmes soit disponible, la DGS révisera son processus interne. Entre autres choses, elle explorera la possibilité de déterminer manuellement quels sont les systèmes de grande importance au sein de l'ARC. Cela nécessiterait un cycle d'examen des autorisations plus fréquent , l'examen de la validité des autorisations des systèmes et la communication trimestrielle des renseignements qui en découlent au Conseil des risques en matière de cybersécurité aux fins d'information et de prise de décisions.

La date d'achèvement cible pour ce plan d'action est mars 2023.

3.2. Surveillance et établissement de rapports

3.2.1 Les activités de surveillance et les mécanismes d'établissement de rapports de surveillance pour l'évaluation et l'autorisation de la sécurité sont définis et exécutés, mais d'autres améliorations doivent être apportées aux indicateurs de rendement clés et aux procédures de surveillance.

La surveillance et l'établissement de rapports sont essentiels pour informer les responsables désignés de l'organisation de l'état actuel de la protection de l'ARC. Les instruments de politique d'entreprise de l'ARC indiquent qu'une approche efficace des contrôles de sécurité axée sur les risques doit être établie, surveillée, maintenue et révisée, et que des mesures correctives doivent être prises rapidement lorsque des problèmes sont décelés. Ces exigences comprennent la définition des responsabilités pour surveiller et établir des rapports sur les décisions concernant le risque résiduel pour l'ARC, l'état de tous les plans de mise en œuvre des mesures de protection et, l'observation et l'efficacité continue des contrôles de sécurité au moyen de vérifications et d'examens périodiques.

L'équipe de vérification interne a noté que les responsabilités et les activités de surveillance pour l'évaluation et l'autorisation de la sécurité ont été définies de manière générale et incluses dans les instruments de politique d'entreprise. L'équipe de vérification interne a également observé que la DGS produit des rapports de surveillance périodiques sur la sécurité de la TI pour la DGI et le Conseil de direction. Des indicateurs de rendement clés spécifiques sont définis et, l'état et la progression des risques et des plans de mise en œuvre des mesures de protection sont fondés sur les recommandations des évaluations de la sécurité et sont communiqués.

Toutefois, l'équipe de vérification interne a constaté qu'il y avait un manque de bases de référence ou de procédures de surveillance définies pour s'assurer que tous les risques ont été repérés et que les plans de mise en œuvre des mesures de protection ont été achevés en temps voulu afin de s'assurer que les risques résiduels dans la production soient traités et signalés lorsqu'ils ne respectent pas les échéanciers ou nécessitent un examen plus approfondi. L'équipe de vérification a également déterminé que ce ne sont pas tous les risques surveillés qui ont été attribués aux inventaires de risques appropriés, en particulier les risques hérités des systèmes, des plateformes et de l'infrastructure de soutien, y compris les risques liés aux fournisseurs de services infonuagiques. De plus, au moment de la vérification, il n'y avait aucune fonction ou procédure en place pour effectuer des examens ou des vérifications qui permettraient de s'assurer que le processus d'évaluation et d'autorisation de la sécurité soit suivi ou pour assurer l'efficacité continue des contrôles de sécurité pour toutes les applications, les composantes et les systèmes requis pour répondre aux exigences de sécurité.

La DGS prévoit mettre sur pied, en tant qu'organe de gouvernance, le Conseil des risques en matière de cybersécurité, qui n'était pas en place au moment de la fin de la vérification, afin de gérer les décisions sur les risques pour la sécurité organisationnelle.

Les lacunes dans les activités de surveillance relatives à la gestion des risques et à l'assurance de l'observation pourraient avoir un impact négatif sur la confidentialité, l'intégrité et la disponibilité des renseignements protégés.

Recommandation 7

La DGS devrait élaborer des mécanismes de surveillance pour assurer l'achèvement en temps opportun des plans de mise en œuvre des mesures de protection, l'établissement de rapports sur la conformité du processus d'évaluation et d'autorisation de la sécurité, et l'efficacité continue des contrôles de sécurité.

Plan d'action 7

La DGS a conçu un Conseil des risques en matière de cybersécurité qui n'a pas encore été officiellement approuvé. Elle devra fournir les données sur les risques en amont et coordonner les mesures d'atténuation des risques avec les propriétaires de systèmes, dans le but d'atténuer rapidement les risques avant qu'ils ne parviennent au Conseil des risques en matière de cybersécurité.

La DGS examinera et implémentera les indicateurs de rendement clés et les flux de travail pour que le Conseil des risques en matière de cybersécurité puisse rendre des comptes sur l'achèvement de la mise en œuvre des mesures de protection par rapport aux délais établis, sur la conformité au processus d'évaluation et d'autorisation de la sécurité, et sur l'efficacité des contrôles de sécurité.

La date d'achèvement cible pour ce plan d'action est mars 2023.

4. Conclusion

Globalement, l'équipe de la vérification interne a constaté que le processus d'évaluation et d'autorisation de la sécurité ainsi que les exigences relatives aux systèmes de renseignements étaient en place pour les évaluations de la sécurité. Toutefois, elle a constaté que des améliorations sont nécessaires pour renforcer davantage les instruments de politique d'entreprise, les rôles et les responsabilités, l'autorisation, la surveillance des indicateurs de rendement et l'élaboration de procédures et d'outils officiels afin de répondre aux besoins de l'ARC.

5. Remerciements

Pour conclure, nous souhaitons reconnaître et remercier la DGS, la DGI, la Direction générale de cotisation, de prestation et de service la Direction générale des appels, la Direction générale des recouvrements et de la vérification et la Direction générale des programmes d'observation pour le temps consacré et les renseignements fournis dans le cadre de cette mission.

6. Annexes

Annexe A : Critères et méthodologie de la vérification

Selon l'évaluation des risques de la Direction générale de la vérification, de l'évaluation et des risques, les secteurs d'intérêt suivants ont été cernés :

Secteurs d'intérêt	Critères
Observation	Les politiques, directives, normes et procédures de l'ARC liées à l'évaluation et à l'autorisation de la sécurité sont en place, à jour, communiquées aux intervenants et en harmonie avec celles du gouvernement du Canada.
	Les rôles et les responsabilités liés à l'évaluation et à l'autorisation de la sécurité sont définis, communiqués et compris par les intervenants.
	Les systèmes, les composantes et les applications sont gérés, évalués et autorisés avec l'acceptation officielle des risques par les intervenants, conformément aux instruments de politique de l'ARC liés à l'évaluation et à l'autorisation de la sécurité.
Surveillance et établissement de rapports	Les indicateurs de rendement de l'évaluation et de l'autorisation de la sécurité sont définis et font l'objet d'un rapport comprenant des mises à jour continues de la conformité à l'intention de la gestion.
	Des mécanismes d'établissement de rapports de surveillance pour l'évaluation et l'autorisation de la sécurité sont en place et fonctionnent comme prévu.

Méthodologie

La méthodologie d'examen comprenait :

- examiner et analyser les instruments de politique d'entreprise et les documents justificatifs liés à l'évaluation et à l'autorisation de la sécurité;
- mener des entrevues et des revues avec la gestion de la DGS et de la DGI, et avec les responsables opérationnels et le personnel de certaines directions générales;
- vérifier la conformité des contrôles au moyen d'examens de la documentation;
- examiner et analyser les données provenant des applications et des outils de sécurité connexes;
- examiner et analyser les indicateurs de rendement et les rapports de surveillance liés à l'évaluation et à l'autorisation de la sécurité.

Annexe B : Glossaire

Terme	Définition
Autorisation d'exploitation	Déclaration officielle d'une autorité d'approbation désignée qui autorise l'exploitation d'un système ou d'un service qui passe à la production et qui accepte expressément les risques pour les opérations de l'ARC. La signature de l'autorisation d'exploitation atteste que le système a satisfait à toutes les exigences en matière de sécurité pour devenir opérationnel.
Disponibilité	Capacité pour les bonnes personnes d'accéder aux bons renseignements ou aux bons systèmes, selon les besoins. La disponibilité est appliquée aux biens d'information, aux logiciels et au matériel (l'infrastructure et ses composantes). La disponibilité implique la protection des biens contre l'accès non autorisé et la compromission.
Infonuagique	Utilisation de serveurs à distance hébergés sur Internet. L'infonuagique permet aux utilisateurs d'accéder à un bassin partagé de ressources informatiques (p. ex., réseaux, serveurs, applications, services) sur demande et depuis n'importe où. Les utilisateurs accèdent à ces ressources par l'intermédiaire d'un réseau informatique au lieu de stocker et de conserver toutes les ressources sur leur ordinateur local.
Confidentialité	Capacité de protéger les renseignements de nature délicate contre l'accès par des personnes non autorisées.
Cyberattaque	Utilisation de moyens électroniques pour interrompre, manipuler ou détruire un système informatique, un réseau ou un appareil, ou obtenir un accès non autorisé à ceux-ci.
Cybermenace	L'utilisation d'Internet pour profiter d'une vulnérabilité connue d'un produit afin d'exploiter un réseau ainsi que les renseignements qui y circulent.
Risque hérité	Risque qu'un système d'information ou une application reçoit de systèmes ou de composantes connexes ou connectés qui sont conçus, installés, évalués, autorisés et surveillés par des entités autres que celles responsables du système ou de l'application (entités internes ou externes à l'organisation où se situe le système ou l'application).
Intégrité	Capacité de protéger les renseignements contre la modification ou la suppression involontaire ou non souhaitable. L'intégrité aide à déterminer que les renseignements correspondent à ce qui est déclaré. Elle s'applique également aux processus opérationnels, à la logique des applications logicielles, au matériel et au personnel.
Risque résiduel	Niveau de risque restant après l'application des mesures de sécurité.

Mesure de protection	Mesure de protection prescrite pour répondre aux exigences en matière de sécurité (c.-à-d. la confidentialité, l'intégrité et la disponibilité) spécifique à un système d'information. Les mesures de protection peuvent comprendre des fonctions de sécurité, des contraintes de gestion, la sécurité du personnel, ainsi que la sécurité des structures physiques, des zones et des appareils.
Plan de mise en œuvre de mesures de protection	Processus utilisé pour effectuer le suivi de la mise en œuvre des recommandations qui ont été déterminées dans une évaluation de la sécurité en vue d'atteindre le niveau voulu de risque résiduel.
Répertoire des applications des solutions	Liste officielle des applications d'entreprise de l'ARC qui rend compte d'une variété de caractéristiques, comme le nom de l'application, l'acronyme, la description, l'entreprise, la technologie et d'autres attributs du portefeuille.
Évaluation de la sécurité	Processus continu d'évaluation des pratiques et des contrôles de sécurité, pour les systèmes et les applications informatiques nouveaux ou existants, visant à déterminer s'ils sont mis en œuvre correctement, fonctionnent comme prévu et produisent les résultats souhaités en ce qui concerne le respect des exigences de sécurité définies.
Autorisation de sécurité	Processus continu visant à obtenir et à maintenir une décision sur la gestion des risques pour la sécurité et à accepter explicitement le risque résiduel avec l'autorisation d'exploitation, en fonction des résultats de l'évaluation de la sécurité.
Contrôle de sécurité	Exigence de sécurité générale, opérationnelle ou technique spécifique à un système d'information qui vise à protéger la confidentialité, l'intégrité et la disponibilité de ses biens de TI. Les contrôles de sécurité peuvent être appliqués à l'aide de diverses solutions de sécurité, dont des produits, des politiques, des pratiques et des procédures de sécurité.
PROTÉGÉ	PROTÉGÉ
Gestion des risques liés à la sécurité	Principe fondamental selon lequel la sécurité est intégrée à la mise à jour continue des connaissances, à la compréhension, à l'évaluation et à l'atténuation des menaces et des risques, tant à l'interne qu'à l'externe, afin de protéger les employés, les renseignements, les biens et les revenus.
Évaluation de la menace et des risques	Processus qui consiste à inventorier les systèmes et à déterminer comment ces biens peuvent être compromis ainsi qu'à évaluer le niveau de risque que les menaces représentent pour les biens, et à recommander des mesures de sécurité pour atténuer les menaces.

Vulnérabilité	Défaut ou faiblesse dans la conception ou l'installation d'un système d'information ou de son environnement qui pourrait être exploité pour compromettre les biens ou les activités d'une organisation.