Vérification interne – Système de gestion de la fraude d'entreprise

Rapport final

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

Agence du revenu du Canada | Canada Revenue Agency

Canada

No de catalogue Rv4-218/2026F-PDF

ISBN 978-0-660-97632-7

Le présent document es disponible sur le site

Web du gouvernement du Canada à

www.canada.ca

Table des matières

Résumé exécutif **3**
Sommaire des recommandations 3
Réponse de la direction 4
Introduction **5**
Point de mire de la vérification interne **6**
Importance 6
Objectif 6
Portée 6
Critères et méthodologie de la vérification interne 7
Constatations, recommandations et plans d'action **7**
Observation 7
Surveillance 12
Remerciements **15**
Annexes **16**
Annexe A : Critères et méthodologie de la vérification interne 16
Annexe B : Glossaire 18

Résumé exécutif

L'Agence du revenu du Canada (ARC) prend très au sérieux la protection des renseignements fiscaux des Canadiennes et Canadiens, et la confiance des particuliers et des entreprises envers l'ARC est la pierre angulaire du régime fiscal du Canada.

En 2017, l'ARC a mis en œuvre le Système de gestion de la fraude d'entreprise (SGFE) afin de réduire davantage les risques d'accès non autorisé aux renseignements des contribuables tout en appuyant la culture d'intégrité de l'ARC. Ce système vérifie en temps réel que les employés accèdent aux renseignements des contribuables uniquement pour exécuter la charge de travail et les tâches qui leur sont attribuées, et alerte la Direction générale de la sécurité lorsque des accès douteux se produisent.

L'objectif de la vérification interne consistait à fournir au commissaire, à la direction de l'ARC et au Conseil de direction (Conseil) l'assurance que le SGFE fonctionne comme prévu en consignant, en gérant, en surveillant et en signalant les activités des utilisateurs conformément aux instruments de politique de l'ARC.

Dans l'ensemble, la vérification interne a permis de conclure que le SGFE fonctionne comme prévu. La vérification interne a également permis de cerner certains aspects qui pourraient être améliorés afin que le SGFE soit en mesure de mieux répondre aux besoins de l'ARC.

La vérification interne a révélé ce qui suit :

- Le processus actuel d'intégration des applications du système bénéficierait d'un cadre d'évaluation des risques plus structuré.
- Il y a des incohérences dans la surveillance des modifications apportées aux règles opérationnelles, et ces modifications ne font pas l'objet d'un suivi afin de déterminer les répercussions sur l'ARC.
- Un processus de téléchargement des registres dans le SGFE est en place. Toutefois, cela n'est pas toujours fait en temps opportun et de façon contrôlée.
- Bien que certains renseignements sur le rendement fassent actuellement l'objet de rapports, ces mesures pourraient être améliorées afin de prendre de meilleures décisions liées aux opérations du SGFE.

Sommaire des recommandations

- La Direction générale de la sécurité devrait consigner les évaluations officielles des risques avant l'intégration afin d'assurer une évaluation des risques appropriée en tenant compte du niveau d'effort lié à l'intégration des applications.
- La Direction générale de la sécurité devrait effectuer la surveillance et le suivi des modifications apportées aux règles opérationnelles, [contenu caviardé]
- La Direction générale de la sécurité, en collaboration avec la Direction générale de l'informatique, devrait créer un processus officiel pour la réingestion des

registres dans le SGFE, y compris les délais et les procédures prévus pour aviser les utilisateurs touchés.
- La Direction générale de la sécurité devrait élaborer des indicateurs de rendement clés afin de mieux comprendre l'efficience et l'efficacité du SGFE.

Réponse de la direction

La Direction générale de la sécurité accepte les recommandations formulées dans ce rapport et a 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

L'Agence du revenu du Canada (ARC) a pour mandat d'administrer les programmes d'impôt et de prestations et les programmes connexes, ainsi que d'assurer le respect des lois établies. L'ARC prend très au sérieux la protection des renseignements fiscaux des Canadiennes et Canadiens, et la confiance des particuliers et des entreprises envers l'ARC est la pierre angulaire du régime fiscal volontaire du Canada. Les employés de l'ARC traitent l'un des plus importants répertoires de renseignements personnels et financiers au pays. La protection de ces renseignements est essentielle à la préservation de l'intégrité et de la réputation de l'ARC.

Afin de veiller à ce que toutes les solutions et les applications, ainsi que tous les systèmes de l'ARC qui permettent aux employés de consulter les renseignements sur les contribuables soient sécurisés, il y a des contrôles de sécurité en place, tels que des outils et des activités de détection, d'enregistrement et de prévention. En 2017, l'ARC a mis en œuvre le Système de gestion de la fraude d'entreprise (SGFE) afin de réduire davantage les risques d'accès non autorisé aux renseignements des contribuables tout en appuyant la culture d'intégrité de l'ARC. Le SGFE permet de cerner de façon proactive les activités douteuses des utilisateurs à l'aide de règles opérationnelles. Le système permet à l'ARC de vérifier en temps réel que les employés accèdent uniquement aux renseignements requis pour exécuter la charge de travail et les tâches qui leur sont attribuées.

En plus de la surveillance en temps réel, le SGFE surveille les accès des employés au moyen de registres de pistes de vérification. Toute mesure prise par un employé sur une solution, un système ou une application de l'ARC donnant accès aux renseignements sur les contribuables est assujettie aux registres de piste de vérification. Ces registres de piste de vérification sont regroupés dans le Système national de pistes de vérification, qui comprend des bandes virtuelles aux fins de stockage et d'historique. Au besoin, la direction peut demander une piste de vérification dans le cadre d'un examen proactif des activités électroniques de ses employés.

Au sein de la Direction générale de la sécurité, la Section des solutions de gestion de la fraude interne est responsable de s'assurer que toutes les solutions et les applications, ainsi que tous les systèmes de l'ARC donnant accès aux renseignements des contribuables sont assujettis à des contrôles de sécurité. La Section des solutions de gestion de la fraude interne tient à jour et améliore le SGFE, saisit et enregistre les transactions des employés effectuées sur les renseignements des contribuables dans les solutions, les systèmes et les applications de l'ARC, et elle appuie les développeurs de systèmes de l'ARC pour s'assurer qu'ils respectent les exigences en matière de sécurité des renseignements.

Également au sein de la Direction générale de la sécurité, la Division des affaires internes est responsable d'examiner les allégations ou les soupçons d'inconduite des employés, y compris les alertes générées par le SGFE. La Division des affaires internes évalue les alertes et détermine s'il faut aller de l'avant avec une enquête préliminaire.

Après avoir mené une enquête préliminaire, la Division des affaires internes détermine si une enquête officielle est justifiée.

Au sein de la Direction générale de l'informatique (DGI), la Section des services de gestion de la fraude d'entreprise est responsable de la maintenance du SGFE au sein de l'ARC.

Depuis sa mise en œuvre, le SGFE a généré plus de 17 000 alertes. Au cours de l'exercice 2022 à 2023, le SGFE a généré 2 334 alertes. Au cours de l'exercice 2023 à 2024, le SGFE a généré 1 850 alertes.

Point de mire de la vérification interne

La présente vérification interne a fait partie du Plan d'assurance et de consultation axé sur les risques de 2023-2024, qui a été approuvé par le Conseil de direction (Conseil) en mars 2023. La vérification interne a été lancée en février 2024, et le cahier de planification a été approuvé par le commissaire en septembre 2024.

Importance

La présente vérification interne est importante parce qu'elle appuie la priorité de l'ARC consistant à renforcer la sécurité et la protection des renseignements personnels. Le Système de gestion de la fraude d'entreprise (SGFE), en tant que contrôle, protège les biens d'entreprise et la réputation de l'ARC, assure l'intégrité des données et est bien harmonisé avec les buts et les objectifs opérationnels actuels et futurs de l'ARC.

Objectif

L'objectif de la vérification interne consistait à fournir au commissaire, à la direction de l'ARC et au Conseil l'assurance que le SGFE fonctionne comme prévu en consignant, en gérant, en surveillant et en signalant les activités des utilisateurs conformément aux instruments de politique de l'ARC.

Portée

La vérification interne a porté sur les processus liés au SGFE, comme la saisie du registre des pistes de vérification et la réception des alertes. La vérification interne ne comprenait pas les processus qui ont lieu après qu'une alerte du SGFE a été sélectionnée par la Division des affaires internes, et les événements subséquents (c'est-à-dire les enquêtes et les mesures disciplinaires).

La période visée par cette vérification s'est étendue du 1er avril 2021 au 31 mars 2024, mais elle a également tenu compte des activités pertinentes depuis la mise en œuvre du SGFE en 2017.

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 entre juillet 2024 et décembre 2024.

La vérification interne 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.

Constatations, recommandations et plans d'action

Observation

L'intégration des demandes dans le SGFE

Le processus actuel d'intégration des applications bénéficierait d'un cadre d'évaluation des risques plus structuré. [contenu caviardé] **pour évaluer et établir l'ordre de priorité de l'intégration des applications dans le Système de gestion de la fraude d'entreprise (SGFE).**

Contexte

Pour que les applications de technologie de l'information (TI) soient surveillées dans le SGFE, une application est soumise au processus d'intégration. [contenu caviardé] La Section des solutions de gestion de la fraude interne effectue le mappage avec l'aide de la DGI.

[contenu caviardé]

L'équipe de la vérification s'attendait à ce que les politiques et les procédures d'intégration des applications soient documentées et accessibles, et qu'elles comprennent un cadre officiel d'évaluation des risques. L'équipe de la vérification s'attendait à ce que les évaluations permettent de déterminer les risques associés aux applications individuelles, les avantages prévus de l'intégration des applications, ainsi que les répercussions sur les ressources et le temps associées à l'intégration des applications.

Constatations

La vérification a permis de conclure qu'il existe un processus et des procédures d'intégration. Toutefois, il n'y a pas de cadre officiel d'évaluation des risques ou de procédures d'estimation du temps en place pour l'intégration des applications.

[contenu caviardé] [redacted] Les priorités d'intégration sont fondées principalement sur [contenu caviardé] [redacted], le niveau de risque conformément aux discussions avec la Division des affaires internes et la Division de l'évaluation de risque lié au personnel, et toutes limites de surveillance déterminées.

La Section des solutions de gestion de la fraude interne consigne ses décisions d'intégration dans des documents Microsoft Word et des courriels stockés sur des lecteurs partagés. Toutefois, aucune estimation officielle du temps n'est établie ou suivie. L'équipe de la vérification a été informée que [contenu caviardé] [redacted]

La Section des solutions de gestion de la fraude interne a indiqué à l'équipe de la vérification qu'il y a une certaine souplesse dans l'intégration si les exigences exigent que des ressources soient nécessaires pour mapper des écrans supplémentaires.

Pourquoi est-ce important?

Un cadre d'évaluation des risques plus exhaustif et une documentation détaillée peuvent prévenir les situations qui pourraient mener à l'intégration d'applications à faible risque, tout en omettant les applications à risque plus élevé, qui sont plus susceptibles de faire l'objet d'une fraude interne ou d'une utilisation malveillante.

Recommandation no 1

La Direction générale de la sécurité devrait consigner les évaluations officielles des risques avant l'intégration des applications afin d'assurer une évaluation des risques appropriée en tenant compte du niveau d'effort lié à l'intégration des applications.

Plan d'action no 1

La Direction générale de la sécurité reconnaît que l'amélioration du cadre d'évaluation des risques existant pour l'intégration des applications dans le Système de gestion de la fraude d'entreprise permettra d'améliorer le processus d'examen annuel. Ce cadre intégrera l'évaluation des risques et tiendra compte du niveau d'effort requis au cours de la phase d'évaluation.

La Direction générale de la sécurité travaillera avec la Section du centre d'expertise en gestion des risques de la Direction générale de la vérification, de l'évaluation et des risques afin d'élaborer un modèle d'établissement des priorités fondé sur les risques pour l'intégration des applications.

La Direction générale de la sécurité, en consultation avec la Section des services de gestion de la fraude d'entreprise de la Direction générale de l'informatique, déterminera les ressources et le niveau d'effort requis pour l'intégration des applications.

La date d'achèvement cible pour ce plan d'action est mai 2026.

Règles opérationnelles

Il y a des incohérences dans la surveillance de l'examen des modifications apportées aux règles opérationnelles, et ces modifications ne font pas l'objet d'un suivi afin de déterminer les répercussions possibles sur l'ARC.

Contexte

Les règles opérationnelles sont des critères définis pour repérer les comportements suspects. Les règles opérationnelles sont programmées dans le SGFE, et lorsqu'il y a une violation d'une règle opérationnelle, le SGFE crée une alerte. Trois équipes différentes (propriétaires de règle opérationnelle) au sein de la Direction générale de la sécurité sont actuellement responsables [contenu caviardé] de règles opérationnelles.

L'équipe de la vérification s'attendait à ce qu'un processus de suivi, d'examen et de mise à jour des règles opérationnelles du SGFE soit en place. L'équipe de la vérification s'attendait également à ce qu'un groupe soit responsable de la surveillance des règles opérationnelles, en veillant à ce que des examens réguliers des règles opérationnelles soient effectués et en tenant des registres des règles opérationnelles [contenu caviardé].

L'équipe de la vérification a analysé les données du SGFE afin de déterminer les principaux jalons des alertes : le moment où l'incident a eu lieu, le moment où l'incident

a été déterminé, le moment où l'alerte a été créée et le moment où l'alerte a été sélectionnée. L'analyse des données a également permis à l'équipe de la vérification de déterminer à quel moment les règles opérationnelles étaient [contenu caviardé] ainsi que le nombre d'incidents et d'alertes créés par chaque règle opérationnelle.

Constatations

La vérification a permis de conclure que les règles opérationnelles sont mises à jour de façon ponctuelle par chaque propriétaire de règle opérationnelle. Dans le cadre de la création de règles ou de leur mise à jour, seulement l'un des trois propriétaires de règles opérationnelles a régulièrement fait appel à des experts en la matière des secteurs de programme et des évaluations du risque de fraude interne pour élaborer de nouvelles règles opérationnelles et modifier celles existantes. La participation d'experts en la matière a été affectée par le degré de complexité de la règle, les propriétaires des règles opérationnelles ayant décidé que les règles plus simples ne nécessitaient pas l'apport des experts. Comme chaque propriétaire de règle opérationnelle décidait de la façon et du moment de mettre en œuvre les modifications aux règles opérationnelles, certaines règles opérationnelles n'ont pas été examinées ou modifiées, même lorsqu'il en découlait un nombre élevé de fausses alertes positives.

Il n'y a pas de registre centralisé de toutes les règles opérationnelles qui mettait en évidence les modifications apportées [contenu caviardé]. La vérification a également révélé que chaque propriétaire tenait à jour sa propre liste de règles opérationnelles [contenu caviardé] du SGFE. La Section des solutions de gestion de la fraude interne fait le suivi [contenu caviardé] de règles opérationnelles, ainsi que de la date à laquelle la règle opérationnelle a été modifiée pour la dernière fois. [contenu caviardé]

En raison des limites actuelles du système, les renseignements détaillés sur les modifications apportées aux règles opérationnelles ne sont pas conservés. L'équipe de la vérification a analysé les données du SGFE afin de déterminer le moment auquel les règles opérationnelles ont généré des alertes. Grâce à cette analyse, l'équipe de la vérification a été en mesure de déterminer le moment auquel les règles opérationnelles ont été [contenu caviardé], divisées et recréées. En travaillant avec la Section des solutions de gestion de la fraude interne et grâce à leur documentation, l'équipe de la vérification a ensuite été en mesure de déterminer la raison pour laquelle ces règles opérationnelles ont été [contenu caviardé] ainsi que les nouvelles règles opérationnelles qui ont été créées Sans l'aide de la Section des solutions de gestion de la fraude interne, l'équipe de la vérification n'aurait pas pu déterminer à partir des données du système le moment auquel les règles opérationnelles [contenu caviardé]

Pourquoi est-ce important?

[contenu caviardé]

[contenu caviardé]

Recommandation no 2

La Direction générale de la sécurité devrait effectuer la surveillance et le suivi des modifications apportées aux règles opérationnelles, [contenu caviardé]

Plan d'action no 2

La Direction générale de la sécurité reconnaît l'importance d'effectuer la surveillance et le suivi des modifications apportées aux règles opérationnelles, [contenu caviardé], et a déjà pris des mesures pour une partie de cette recommandation.

Une zone « Note » en format libre a été ajoutée à chaque règle opérationnelle dans le Centre d'enquête du Système de gestion de la fraude d'entreprise (SGFE). Les utilisateurs du SGFE qui ont accès à la modification des règles dans le SGFE ont reçu la directive d'entrer une note normalisée lorsqu'ils modifient une règle opérationnelle . La zone de note comprendra les détails de la modification de la règle, la date de la modification et l'ID utilisateur de l'utilisateur qui entre la note. Cela servira de registre centralisé de toutes les règles, des modifications apportées aux règles [contenu caviardé]

La Section des solutions de gestion de la fraude interne établira des définitions exploitables pour les résolutions des alertes afin d'aider la Division des affaires internes à sélectionner systématiquement la résolution la plus appropriée pour chaque alerte. Cela favorisera une meilleure interprétation des données et un meilleur processus décisionnel.

Les règles opérationnelles avec une résolution plus élevée en faux positifs seront examinées et, s'il y a lieu, une mesure [contenu caviardé] peut être prise.

La date d'achèvement cible pour ce plan d'action est mai 2026.

Surveillance

Téléchargement des dossiers de piste de vérification

Un processus de téléchargement des registres dans le SGFE est en place. Toutefois, cela n'est pas toujours fait en temps opportun et de façon contrôlée.

Contexte

[contenu caviardé]

L'équipe de la vérification s'attendait à ce qu'un processus officiel soit en place pour le téléchargement des registres et qu'il soit effectué en temps opportun et de façon contrôlée.

Constatations

L'équipe de la vérification a conclu qu'un processus est en place pour le téléchargement des registres dans le SGFE. Dans le cadre de ce processus, le nombre prévu de registres téléchargés dans le SGFE est mappé avec les registres créés dans les registres de piste de vérification.

La DGI fait le suivi [contenu caviardé] du nombre de registres qui auraient dû être téléchargés dans le SGFE et du nombre réel de registres qui ont été téléchargés. [contenu caviardé] La DGI ajoute également des notes indiquant les dates auxquelles la réingestion a eu lieu et tout problème correspondant qui a causé le téléchargement infructueux des registres. [contenu caviardé]

[contenu caviardé]

[contenu caviardé]

[contenu caviardé]

Pourquoi est-ce important?

Un retard dans la création d'alertes par la SGFE et la réception d'alertes par la Division des affaires internes pourrait entraîner des retards dans la détection des accès non autorisés et des fraudes, ainsi que dans les mesures prises pour y remédier. Un téléchargement et une réingestion plus contrôlés et en temps opportun des registres dans le SGFE permettraient de détecter la fraude et d'y répondre de manière plus efficace et plus rapidement.

Recommandation no 3

La Direction générale de la sécurité, en collaboration avec la Direction générale de l'informatique, devrait créer un processus officiel pour la réingestion des registres dans le Système de gestion de la fraude d'entreprise, y compris les délais et les procédures prévus pour aviser les utilisateurs touchés.

Plan d'action no 3

La Direction générale de la sécurité, en collaboration avec la Direction générale de l'informatique (DGI), créera un processus officiel pour la réingestion des registres dans le Système de gestion de la fraude d'entreprise (SGFE).

[contenu caviardé]

La Section des SGFI maintiendra une communication uniforme au sujet des activités de réingestion avec les intervenants afin de les aider à se préparer aux répercussions éventuelles.

Une fois que le travail de réingestion sera terminé, les renseignements seront sauvegardés dans un dossier centralisé géré par la Section des SGFI .

[contenu caviardé]

Mesures du rendement

Il y a des possibilités d'améliorer les mesures du rendement entrées et communiquées aux fins de prise de décisions.

Contexte

L'équipe de la vérification s'attendait à ce que les renseignements sur le rendement soient entrés et utilisés pour orienter les décisions sur les opérations du SGFE en fonction des comportements et des résultats découlant des règles opérationnelles. Certains des renseignements attendus étaient les échéanciers des alertes et les taux de faux positifs des règles opérationnelles. À l'aide de ces renseignements, les décisions visant à améliorer le système ou les règles opérationnelles auraient dû être prises et, par conséquent, l'assurance que le SGFE fonctionne comme prévu aurait été obtenue.

Constatations

L'équipe de la vérification a constaté que les renseignements sur le rendement sont déclarés dans un tableau de bord trimestriel des solutions de gestion de la fraude interne transmis au sein de la Direction générale de la sécurité. Ce tableau de bord rend compte de six indicateurs, y compris les volumes quotidiens et les alertes par région. [contenu caviardé] , ces indicateurs ne sont pas nécessairement utiles au moment de prendre des décisions en matière de programmation, [contenu caviardé]

L'équipe de la vérification a analysé les données du SGFE et a cerné des indicateurs de rendement, comme la résolution des alertes par règle opérationnelle, le temps écoulé entre l'incident et la création de l'incident, et le temps écoulé entre l'incident et la création de l'alerte, ce qui pourrait mieux informer la direction sur les priorités pour [contenu caviardé]

Pourquoi est-ce important?

Les renseignements sur le rendement appuient la prise de décisions liées aux règles opérationnelles [contenu caviardé]. Sans indicateurs de rendement significatifs, il est difficile de comprendre le rendement du SGFE.

Recommandation no 4

La Direction générale de la sécurité devrait élaborer des indicateurs de rendement clés qui peuvent être utilisés afin de mieux comprendre l'efficience et l'efficacité du Système de gestion de la fraude d'entreprise.

Plan d'action no 4

La Direction générale de la sécurité s'engage à examiner, améliorer et mettre à jour les indicateurs de rendement clés existants.

La Section des solutions de gestion de la fraude interne définira les valeurs de résolution des alertes à la disposition des utilisateurs du Système de gestion de la fraude d'entreprise (SGFE) à la suite de leur examen d'une alerte. Cela aidera à améliorer la qualité et la fiabilité des données, ce qui contribuera à une interprétation et à une prise de décisions plus exactes.

La Section des solutions de gestion de la fraude interne recueillera et analysera ensuite les valeurs de résolution des alertes sélectionnées par les utilisateurs du SGFE, ce qui donnera un aperçu du rendement et de l'efficacité des modèles de détection. Cette analyse permettra de rendre compte du rendement des opérations du SGFE.

La date d'achèvement cible pour ce plan d'action est mai 2026.

Remerciements

Pour conclure, la Direction générale de la vérification, de l'évaluation et des risques souhaite reconnaître et remercier la Direction générale de la sécurité et la Direction générale de l'informatique 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 Direction générale de la vérification, de l'évaluation et des risques, les secteurs d'intérêt suivants ont été cernés :

Secteurs d'intérêt	Critères
Observation	Un processus est en place pour l'intégration des applications dans le Système de gestion de la fraude d'entreprise (SGFE).
	Des processus sont en place pour examiner et modifier les modèles de détection (règles opérationnelles).
Surveillance	Les alertes du SGFE sont reçues en temps opportun.
	Des mesures de rendement sont en place et fournissent des renseignements exacts et pertinents pour appuyer la prise de décision.

Méthodologie de la vérification interne

- **Examen de la documentation**: examiner la documentation des directions générales et des secteurs de programmes afin de s'assurer que les plans, les politiques, et les procédures sont documentés, communiqués, et suivis. Les secteurs suivants sont inclus dans la portée :
    - Direction générale de la sécurité: Division de la sécurité de l'information, Division des affaires internes, Division de l'évaluation de risque lié au personnel
    - Direction générale de l'informatique (DGI): Division de développement et opérations des solutions de sécurité

- **Analyse de données** : mener une analyse détaillée de la base de données du SGFE et élaborer des tests analytiques, et communiquer les résultats de ces tests avec la Direction générale de la sécurité et la DGI aux fins de validation.
- **Entrevues** : mener des entrevues auprès des équipes sélectionnées au sein de la Direction générale de la sécurité, la DGI, et la Direction générale des affaires publiques.

Annexe B : Glossaire

Terme	Définition
Registre de piste de vérification	Un registre de toute mesure prise par un employé à l'égard d'une solution, d'un système ou d'une application de l'ARC, qui lui permet de consulter, de modifier, de créer, de supprimer, de rechercher ou de sélectionner des renseignements sur les contribuables.
Règles opérationnelles	Logique et conditions prédéfinies qui aident à détecter, à prévenir et à réagir aux activités frauduleuses au sein de l'ARC. Ces règles définissent la façon dont les transactions, les comportements des utilisateurs et les interactions du système sont surveillés afin de cerner les risques de fraude potentiels.
Système de gestion de la fraude d'entreprise (SGFE)	Une plateforme logicielle intégrée conçue pour détecter, prévenir et gérer les activités frauduleuses dans l'ensemble des opérations de l'ARC. Les solutions du SGFE fournissent une surveillance en temps réel des transactions, une reconnaissance des modèles, une cotation des risques et des capacités de gestion des cas pour repérer les comportements suspects.
Incident	Lorsque les conditions des règles opérationnelles sont remplies, un incident est généré. Les incidents sont évalués selon un modèle de cotation prédéfini, qui détermine la gravité de l'incident.
Mappage	L'examen des écrans d'une application et la détermination des renseignements sur les contribuables et les zones qui doivent être mappées afin que les règles opérationnelles et les alertes puissent être appliquées.
Intégration	Le processus d'intégration et de configuration de nouvelles applications logicielles dans le système de l'ARC. Ce processus permet de s'assurer que l'application est correctement configurée, sécurisée et prête à être utilisée par les utilisateurs prévus.
En temps réel	Le traitement ou la transmission immédiate des données à mesure qu'elles sont reçues, avec peu ou pas de retard perceptible. Ce concept est essentiel dans les scénarios où une réponse en temps opportun est essentielle.

Réingestion	Le processus de téléchargement, d'importation ou de traitement des registres de données dans le SGFE qui ont déjà été ingérés ou téléchargés une fois.