Internal Audit – Enterprise Fraud Management System

Final Report

Audit, Evaluation, and Risk Branch

Canada Revenue Agency | Agence du revenu du Canada

Canada

Catalogue No. Rv4-218/2026E-PDF

ISBN 978-0-660-97631-0

This document is available on the Government of Canada website at www.canada.ca

This document is available in alternative formats upon request.

Table of contents

Executive summary

The Canada Revenue Agency (CRA) takes the protection of Canadians' tax information very seriously, and the confidence that individuals and businesses have in the CRA is a cornerstone of Canada's tax system.

In 2017, the CRA implemented the Enterprise Fraud Management System (EFMS) to further reduce the risks of unauthorized access to taxpayer information while supporting the CRA's culture of integrity. This system verifies in real time that employees only access taxpayer information to carry out their assigned workload and duties and alerts the Security Branch when questionable accesses occur.

The objective of the internal audit was to provide the Commissioner, CRA management, and the Board of Management (Board) with assurance that the EFMS is working as intended by recording, managing, monitoring, and reporting user activities in accordance with CRA policy instruments.

Overall, the internal audit concluded that the EFMS is working as intended. The internal audit also identified some aspects that could be improved so that the EFMS can better meet the CRA's needs.

The internal audit found the following:

- The current system application onboarding process would benefit from a more structured risk assessment framework
- There are inconsistencies in the oversight of business rule changes, and modifications to business rules are not tracked to determine implications to the CRA
- A process is in place for the loading of records into the EFMS; however, it is not always done in a timely and controlled manner
- Although some performance information is currently reported on, these measures could be improved to make better decisions related to EFMS operations

Summary of recommendations

- The Security Branch should document formal risk assessments before onboarding to ensure proper risk evaluation with consideration of the level of effort of onboarding applications
- The Security Branch should monitor and track business rule changes, [redacted content]
- The Security Branch, in conjunction with the Information Technology Branch, should create a formalized process for the re-ingestion of records into the EFMS, including expected timeframes and procedures to advise impacted users
- The Security Branch should develop key performance indicators to better understand the efficiency and effectiveness of the EFMS

Management response

The Security Branch agrees with the recommendations in this report and has developed related action plans. The Audit, Evaluation, and Risk Branch has determined that the action plans appear reasonable to address the recommendations.

Introduction

The Canada Revenue Agency's (CRA) mandate is to administer tax, benefits, and related programs, and to ensure compliance with established legislation. The CRA takes the protection of Canadians' tax information very seriously, and the confidence that individuals and businesses have in the CRA is a cornerstone of Canada's voluntary tax system. CRA employees handle one of the largest repositories of personal and financial information in the country; protecting this information is crucial to upholding the integrity and reputation of the CRA.

To ensure all CRA solutions, systems, and applications that allow for the viewing of taxpayer information by employees are secure, there are security controls in place, such as detection, recording, and prevention tools and activities. In 2017, the CRA implemented the Enterprise Fraud Management System (EFMS) to further reduce the risks of unauthorized access to taxpayer information while supporting the CRA's culture of integrity. The EFMS enables the proactive identification of questionable user activities using business rules. The system enables the CRA to verify in real time that employees are only accessing the information required to carry out their assigned workload and duties.

In addition to real-time monitoring, the EFMS monitors employees' accesses through audit trail records. Any action undertaken by an employee on a CRA solution, system, or application with access to taxpayer information is subject to audit trail records. These audit trail records are consolidated in the National Audit Trail System, which comprises virtual tapes for storage and historical purposes. If and when required, management can request an audit trail as part of a proactive review of their employees' electronic activities.

Within the Security Branch, the Internal Fraud Management Solutions (IFMS) Section is responsible for ensuring all CRA solutions, systems, and applications with access to taxpayer information are subject to security controls. The IFMS Section maintains and enhances the EFMS, captures and records employees' transactions carried out on taxpayer information on CRA solutions, systems, and applications, as well as supports CRA system developers to ensure the developers meet information security requirements.

Also within the Security Branch, the Internal Affairs Division is responsible for reviewing allegations or suspicions of employee misconduct, including alerts generated by the EFMS. The Internal Affairs Division assesses the alerts and determines whether to move ahead with a preliminary investigation. After conducting a preliminary investigation, the Internal Affairs Division then determines whether a formal investigation is warranted.

Within the Information Technology Branch (ITB), the Enterprise Fraud Management Services Section is responsible for maintaining the EFMS within the CRA.

Since its implementation, the EFMS has generated over 17,000 alerts. In fiscal year 2022 to 2023, the EFMS generated 2,334 alerts. In fiscal year 2023 to 2024, the EFMS generated 1,850 alerts.

Focus of the internal audit

This internal audit was included in the 2023-2024 Risk-Based Assurance and Advisory Plan, which was approved by the Board of Management (Board) in March 2023. The internal audit launched in February 2024, and the Assignment Planning Memorandum was approved by the Commissioner in September 2024.

Importance

This internal audit is important because it supports the CRA's priority of strengthening security and safeguarding privacy. The Enterprise Fraud Management System, as a control, protects the CRA's corporate assets and reputation, ensures data integrity, and is well aligned with the CRA's current and future business goals and objectives.

Objective

The internal audit objective was to provide the Commissioner, CRA management, and the Board with assurance that the EFMS is working as intended by recording, managing, monitoring, and reporting user activities in accordance with CRA policy instruments.

Scope

The internal audit covered processes related to the EFMS, such as capturing the audit trail record and receiving the alert. The internal audit did not include processes that occur after an EFMS alert has been screened by the Internal Affairs Division and the subsequent events (in other words, investigation and discipline).

The period covered in this internal audit is from April 1, 2021, to March 31, 2024, but it also considered pertinent activities since the EFMS implementation in 2017.

Internal audit criteria and methodology

The internal audit criteria and methodology can be found in Appendix A.

The examination phase of the internal audit took place from July 2024 to December 2024.

The internal audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing, as supported by the results of the quality assurance and improvement program.

Findings, recommendations, and action plans

Compliance

Onboarding of applications into EFMS

The current application onboarding process would benefit from a more structured risk assessment framework. [redacted content] **to evaluate and prioritize the onboarding of applications into the Enterprise Fraud Management System (EFMS).**

Background

In order for information technology (IT) applications to be monitored in the EFMS, an application goes through the onboarding process. [redacted content] The IFMS Section completes this mapping with the assistance of the ITB.

[redacted content]

The audit team expected that policies and procedures for onboarding applications are documented, accessible, and include a formal risk assessment framework. The audit team expected that assessments identify the risks associated with individual applications, the expected benefits of the applications being onboarded, as well as the resource and time implications associated with onboarding the applications.

Findings

The audit found that there is an onboarding process and procedures. However, there is no formal risk assessment framework or time estimates procedures in place for onboarding applications.

[redacted content] Onboarding priorities are based [redacted content] the level of risk as per

discussions with the Internal Affairs Division and the Personnel Risk Assessment Division, and any identified monitoring limitations.

The IFMS Section records its onboarding decisions in Microsoft Word documents and emails stored on shared drives. However, no formal time estimates are established or tracked. The audit team was told that the [redacted content]

The IFMS Section shared with the audit team that there is flexibility in onboarding if requirements dictate that resources are needed for mapping additional screens.

Why it matters

A more comprehensive risk assessment framework and detailed documentation may prevent situations that could lead to the onboarding of lower-risk applications while omitting higher-risk applications, which are more susceptible to internal fraud or misuse.

Recommendation #1

The Security Branch should document formal risk assessments before onboarding applications to ensure proper risk evaluation with consideration of the level of effort of onboarding applications.

Action Plan #1

The Security Branch recognizes that improving the existing risk assessment framework for onboarding applications to the Enterprise Fraud Management System will enhance the annual review process. This framework will incorporate risk evaluation and consider the level of effort required during the evaluation phase.

The Security Branch will work with the Risk Management Centre of Expertise Section of the Audit, Evaluation, and Risk Branch to develop risk-based prioritization model for onboarding applications.

The Security Branch, in consultation with the Enterprise Fraud Management Services Section of the Information Technology Branch, will determine the level of effort and resources required for onboarding applications.

The target completion date for this action plan is May 2026.

Business Rules

There are inconsistencies in the oversight of the review of business rule changes, and modifications to business rules are not tracked to determine what implications they may have on the CRA.

Background

Business rules are defined criteria for identifying suspicious behaviour. Business rules are programmed in the EFMS, and when there is a violation of a business rule, the EFMS creates an alert. Three different teams (business rule owners) within the Security Branch are currently responsible for the [redacted content] of business rules.

The audit team expected that a process to track, review, and update the EFMS business rules is in place. The audit team also expected to find that a group is responsible for the oversight of the business rules, ensuring that regular reviews of the business rules are conducted and keeping records of the [redacted content] business rules.

The audit team analyzed the EFMS data to identify the key milestones of alerts: when the incident occurred, when the incident was identified, when the alert was created, and when the alert was screened. The data analysis also allowed the audit team to identify when business rules were [redacted content] as well as the number of incidents and alerts that each business rule created.

Findings

The audit found that business rules are updated on an ad-hoc basis by each business rule owner. As part of rule creation or updates, only one of the three business rules owners routinely used subject matter experts from program areas and internal fraud risk assessments to develop new and modify existing business rules. The involvement of subject matter experts was affected by the degree of complexity of the rule, with business rule owners deciding that simpler rules did not require input from the experts. As each business rule owner decided how and when to implement changes to the business rules, some business rules had not been reviewed or modified, even when they were creating a high number of false positive alerts.

There is no centralized record of all business rules that highlighted what changes had been made and [redacted content] The audit also found that each owner maintained their own list of [redacted content] EFMS business rules. The IFMS Section keeps track [redacted content] of business rules, as well as the date the business rule was last modified. [redacted content]

Due to the current system limitations, detailed information on changes to business rules are not maintained. The audit team analyzed the EFMS data to determine when business rules generated alerts. Through this analysis, the audit team was able to identify when business rules were [redacted content], split, and recreated. Working with the IFMS Section and their documentation, the audit team was then able to determine why these business rules were [redacted content] and what new business rules were created [redacted content] Without assistance from the IFMS Section, the audit team could not determine from the system data when business rules [redacted content]

Why it matters

[redacted content]

Recommendation #2

The Security Branch should monitor and track business rule changes, [redacted content]

Action Plan #2

The Security Branch recognizes the importance of monitoring and tracking business rule changes[redacted content], and has already taken action for part of this recommendation.

A freeform “Note” field has been added to each business rule in the Investigation Centre of the Enterprise Fraud Management System (EFMS). EFMS users with access to modify the rules in EFMS have been instructed to enter a standardized note when they change a business rule [redacted content] The note field will include details of the rule change, the date of the change, and the user ID of the user entering the note. This will serve as a centralized record of all rules, changes to the rules, [redacted content]

The Internal Fraud Management Solutions Section will establish actionable definitions for alert resolutions to assist the Internal Affairs Division in consistently selecting the most suitable resolution for each alert. This will foster better data interpretation and decision making.

The business rules with higher false positive resolution will be reviewed and, if appropriate, an action [redacted content] may be taken.

The target completion date for this action plan is May 2026.

Monitoring

Loading of Audit Trail Records

A process is in place for the loading of records into the EFMS. However, it is not always done in a timely and controlled manner.

Background

[redacted content]

The audit team expected that a formal process is in place for the loading of records and that it is done in a timely and controlled fashion.

Findings

The audit team found that a process is in place for the loading of records into the EFMS. As a part of this process, the expected number of records loaded into the EFMS is matched to the records created in the audit trail records.

The ITB [redacted content] tracks the number of records that should have been loaded into the EFMS and the actual number of records that were loaded. [redacted content] The ITB also includes notes indicating the dates that re-ingestion occurred and any corresponding issues that caused the incorrect loading of records. [redacted content]

[redacted content]

[redacted content]

Why it matters

A delay in the EFMS creating alerts and the Internal Affairs Division receiving alerts could lead to delays in detecting and responding to unauthorized access and fraud. A more controlled and timely loading and reloading of records into the EFMS would allow for better and more timely fraud detection and response.

Recommendation #3

The Security Branch, in conjunction with the Information Technology Branch, should create a formalized process for the re-ingestion of records into the Enterprise Fraud Management System, including expected timeframes and procedures to advise impacted users.

Action Plan #3

The Security Branch, in collaboration with the Information Technology Branch (ITB), will create a formalized process for the re-ingestion of records into the Enterprise Fraud Management System (EFMS).

[redacted content]

The IFMS Section will maintain consistent communication about re-ingestion activities with stakeholders to help them prepare for the potential impacts.

Once the re-ingestion work is finalized, the information will be saved in a centralized folder managed by the IFMS Section.

[redacted content]

Performance Measures

There are opportunities to improve the performance measures being captured and reported for decision making.

Background

The audit team expected performance information to be captured and used to inform decisions on EFMS operations based on the behaviours and results of the business rules. Some of the information expected to be seen was the timelines of alerts and the false positive rates of business rules. Using this information, decisions to improve the system or business rules should have been made, and assurance that the EFMS is operating as intended would have been obtained.

Findings

The audit team found that performance information is reported in a quarterly Internal Fraud Management Solutions Dashboard shared within the Security Branch. This

dashboard reports on six indicators, including daily volumes and alerts by region. [redacted content] these indicators are not necessarily useful when making programming decisions [redacted content]

The audit team analyzed EFMS data and identified performance indicators, such as alert resolution by business rule, the time between incident and incident creation, and the time between incident and alert creation, which could better inform management on priorities for [redacted content]

Why it matters

Performance information supports decision making related to business rules [redacted content] Without meaningful performance indicators, it is difficult to understand how well the EFMS is performing.

Recommendation #4

The Security Branch should develop key performance indicators that can be used to better understand the efficiency and effectiveness of the Enterprise Fraud Management System.

Action Plan #4

The Security Branch is committed to reviewing, improving, and updating the existing key performance indicators (KPI).

The Internal Fraud Management Solutions (IFMS) Section will define the alert resolution values available to Enterprise Fraud Management System (EFMS) users following their review of an alert. This will help improve the quality and reliability of the data, which will contribute to more accurate interpretation and decision making.

The IFMS Section will then collect and analyze the alert resolution values as selected by the EFMS users, which will provide insight into the performance and effectiveness of detection models. This analysis will enable reporting on the performance of the EFMS's operations.

The target completion date for this action plan is May 2026.

Acknowledgement

In closing, the Audit, Evaluation, and Risk Branch would like to acknowledge and thank the Security Branch and the Information Technology Branch for the time dedicated and the information provided during the course of this engagement.

Appendices

Appendix A: Internal audit criteria and methodology

Internal audit criteria

Based on the Audit, Evaluation, and Risk Branch's risk assessment, the following lines of enquiry were identified:

Lines of enquiry	Criteria
Compliance	A process is in place for the onboarding of applications into the Enterprise Fraud Management System (EFMS).
	Processes are in place for reviewing and modifying the detection models (business rules).
Monitoring	EFMS alerts are received in a timely manner.
	Performance measures are in place and provide accurate and relevant information to support decision making.

Internal audit methodology

- **Documentation review**: review documentation from branches and program areas to verify that plans, policies, and procedures are documented, communicated, and followed. The following areas are included in scope:
    - Security Branch: Information Security Division, Internal Affairs Division, Personnel Risk Assessment Division
    - Information Technology Branch (ITB): Security Solutions Operations and Development Division
- **Data analytics**: conduct a detailed analysis of the EFMS database, and develop analytical tests and share the results of these tests with the Security Branch and the ITB for validation.
- **Interviews**: conduct interviews with select teams within the Security Branch, the ITB, and the Public Affairs Branch.

Appendix B: Glossary

Term	Definition
Audit trail record	A record of any action undertaken by an employee on a CRA solution, system, or application that allows them to view, modify, create, delete, search, and/or select taxpayer information.
Business rules	Predefined logic and conditions that help detect, prevent, and respond to fraudulent activities within the CRA. These rules define how transactions, user behaviors, and system interactions are monitored to identify potential fraud risks.
Enterprise Fraud Management System (EFMS)	An integrated software platform designed to detect, prevent, and manage fraudulent activities across CRA's operations. EFMS solutions provide real-time monitoring of transactions, pattern recognition, risk scoring, and case management capabilities to identify suspicious behaviours.
Incident	When business rule conditions are met, an incident is generated. Incidents are evaluated according to a pre-defined scoring model, which determines the severity of the incident.
Mapping	Reviewing application screens and identifying taxpayer information/fields that need to be mapped so that business rules and alerts can be applied.
Onboarding	The process of integrating and setting up new software applications within the CRA's system. This process ensures that the application is properly configured, secure, and ready for use by intended users.
Real time	The immediate processing or transmission of data as it is received, with little to no perceptible delay. This concept is crucial in scenarios where a timely response is essential.
Re-ingestion	The process of loading, importing, or processing data records into the EFMS again after they have already been ingested or loaded once.