Canada Border Services Agency
Agence des services frontaliers du Canada

Canada

Audit of fraud risk management

Canada Border Services Agency

Agence des services frontaliers du Canada

PS38-141/2025E-PDF
ISBN: 978-0-660-79304-7

Aussi disponible en français sous le titre :
Vérification de la gestion des risques de fraude

Audit of fraud risk management

Internal Audit and Program Evaluation Directorate
April 2025

Note: [redacted] appears where sensitive information has been removed in accordance with the *Access to Information Act* and the *Privacy Act*.

Table of contents

- Introduction
- About the audit
- Significance of the audit
- Statement of conformance
- Audit conclusion
- Key findings
- Summary of recommendations
- Management response
- Audit Findings
    - Governing fraud risk management
    - Monitoring fraud risk management
    - Assessing fraud risks
- Appendix A: Audit criteria
- Appendix B: Previous audits
- Appendix C: Fraud related training
- Appendix D: Glossary
- Appendix E: Acronyms

Introduction

The Canada Border Services Agency (hereafter the CBSA or the agency) processes millions of travellers, shipments, duties and taxes every year, as part of its mandate to facilitate the free flow of legitimate trade and travel[1]. As a result, the agency plays a vital role in supporting the economy, national security and public safety of Canada.

[1] 2022-2023 Departmental Result Report: Canada Border Services Agency

What is fraud

Fraud can be defined as an intentional act by one or more individuals among employees, management, those charged with governance (internal) or third parties (external) involving the use of deception to obtain an unjust or illegal advantage[2].

Fraudulent acts that are carried out by persons internal to an organization (employees) is referred to internal fraud or occupational fraud. It is considered a type of misconduct at the CBSA. According to the Association of Certified Fraud Examiners (ACFE), the three main categories of internal fraud are:

- corruption such as receiving bribes
- asset misappropriation such as stealing and/or misusing government property (including information)
- financial statement fraud such as concealing liabilities and expenses[3]

Experts agree that three components, when present, increase the risk of individuals committing fraud: pressure, opportunity, and the ability to rationalize the fraudulent act. These three elements are commonly referred to as the fraud triangle[4].

Fraud, regardless of whether it is alleged or proven, can erode public trust and/or pose a significant risk to the integrity of programs and services. As a result, it is important that organizations put in place processes and practices to help:

- identify where fraud risks are present
- determine the best methods to prevent fraud from taking place
- implement the activities to detect fraud as early as possible
- investigate fraud allegations
- take corrective action when fraudulent activity has been discovered

A fraud risk management program

According to the Committee of Sponsoring Organisations of the Treadway Commission (COSO), a Fraud Risk Management (FRM) Program is an organization’s overall set of processes and procedures for managing its fraud risks[5]. The essential elements of an FRM program include:

- the governance and oversight around FRM as well as the policies that establish the FRM approach, document roles and responsibilities and set the tone at the top
- a fraud risk assessment (FRA) that identifies an organization’s frauds risks and schemes, the amount of exposure to these risks and its approach to address them
- the preventive and detective controls including the processes, procedures, and activities designed and implemented to reduce fraud risk

[2] Guide on Managing Risks at the Office of the Auditor General

[3] 2024 ACFE Report to the Nations

[4] Institute of Internal Auditors The Shapes of Fraud

[5] COSO Fraud Risk Management Guide

- conducting investigations and reporting the results of fraud allegations
- monitoring the FRM performance and using the results to continually improve the entire program[6]

An FRM framework or policy, documents the above elements and also supports the allocation of resources to help implement the organization's defined approach[7].

Fraud risk management at the CBSA

At the CBSA, FRM activities occur across various business areas; however, some of the key areas of accountability lie with the Deputy Head, who establishes the Code of Conduct and fosters a culture of values and ethics, the Chief Security Officer who maintains and oversees the agency's Integrity Program, and conducts investigations on misconduct and the Agency's Financial Comptroller who conducts the FRA.

Some other key areas of responsibility for FRM include (this is not an exhaustive list):

- all employees who must adhere to values and ethics, and report any detected or suspected misconduct (including fraud) involving employees
- management who must establish and oversee internal controls to prevent and detect possible acts of fraud, and ensure they are functioning as intended
- the Values and Ethics Office within the Human Resources Branch, who manages and maintains the CBSA Code of Conduct, and provides recommendations to delegated authorities on conflicts of interest disclosures
- the Senior Officer for Internal Disclosure who receives disclosures of wrongdoing and investigates them where appropriate

About the audit

The audit's objective was to assess the implementation of CBSA's FRM[8] program.

Audit scope inclusions

The period under review for the Audit of Internal Fraud Risk Management was from April 2021 to September 2024. This scope period was chosen to allow an examination of the Agency's two most recent FRAs. The audit examined the following elements (refer to Appendix A, Audit criteria):

- the governance structures and oversight mechanisms for the management of fraud risk
- the FRA
- the management of fraud prevention and detection controls
- monitoring and reporting on FRM activities to support continuous improvement

[6] COSO Fraud Risk Management Guide

[7] COSO Fraud Risk Management Guide

[8] The term "fraud risk management" is being used instead of "fraud management" as was commonly referenced in the 2022 Internal Fraud Management Framework. This is because the management of fraud risk more holistically reflects the management of the activities to both prevent (mitigate the risk of fraud occurring) and detect fraud.

For the purposes of this audit, the above scope areas where possible also considered fraud that can be perpetrated by employees with linkages to parties external to the organization.

Audit scope exclusions

The audit excluded the following areas:

- An assessment of the agency's external FRM processes and practices.
- An examination of the investigations of fraud allegations. This area was recently audited in the 2020 Follow up Audit of Professional Standards.
- Testing of individual prevention and detection controls for the risks identified in the agency's Fraud Risk Profile (FRP). Given the limited time and resources for this engagement, the audit instead examined a non-random sample of four risks to determine whether the Agency has established processes to test the effectiveness of identified controls and how this information is used in the FRP.
- A review of the CBSA's internal audit risk-based audit planning process as well as investigations conducted by the Senior Officer for Internal Disclosure. Both activities fall under the Internal Audit and Program Evaluation Directorate and therefore a review of these activities presented a conflict of interest. While not audited, relevant opportunities were shared with these two areas for further action.

Audit methodology

To conclude on the audit objective, the following methods were used to gather evidence:

- reviewed and analyzed over 450 key documents such as records of decisions, terms of reference of executive governance committees, policies and procedures, fraud risk tools and templates, FRAs, integrated business profiles, training records, annual reports and reporting dashboards
- Interviewed 20+ stakeholders with roles and responsibilities for FRM

Significance of the audit

In fiscal year 2022 to 2023, the CBSA facilitated the cross border movement of 70.5 million travellers, collected 39.7 billion dollars in duties and taxes, processed 132.5 million courier shipments and seized over 16 million dollars worth of currency and monetary instruments[9]. Given the extensive scale of CBSA's operations, fraud, either alleged or proven, can undermine the ability to meet its mandate and deliver services to Canadians. For example, fraudulent acts and their consequences can:

- damage the Agency's reputation and lead to a loss of trust from the Canadian public and its various partners
- lead to significant financial loss either from the act itself, or the effort to investigate, correct and recover from the loss
- interfere with the agency's compliance with legislative and regulatory requirements if systems and processes are compromised

[9] 2022 to 2023 Departmental Results Report: Canada Border Services Agency

- from a human perspective, lead to low employee morale and negatively affect the organizational culture[10].

All of these impacts can divert the agency's time and finite resources from conducting its work.

A number of audits in the last five years have highlighted gaps in the controls of key agency processes such as contracting and procurement, payroll, internal controls for financial reporting and border management (people and goods) that are relevant to FRM (refer to Appendix B, Previous audits). Recommendations to address some of these control gaps are ongoing. Through this audit, the agency assessed its overall FRM program to have a holistic picture of its approach.

This audit was approved in the agency's 2023 Risk-Based Audit and Evaluation Plan.

Statement of conformance

This audit engagement conforms to the Treasury Board's *Policy* and *Directive on Internal Audit* and the Institute of Internal Auditors' (IIA) *International Professional Practices Framework*. Sufficient and appropriate evidence was gathered through various procedures to provide an audit level of assurance. The agency's internal audit function is independent and internal auditors performed their work with objectivity as defined by the IIA's *International Standards for the Professional Practice of Internal Auditing*.

Audit conclusion

An effective FRM program is critical to an organization's success as it can help prevent and lessen the negative impacts that can occur as a result of fraud.

The agency is conducting FRM activities; however, there are gaps in the overall approach that should be addressed in order to continue to improve CBSA's efforts.

The agency has a new Integrity Framework to help support and facilitate a culture of integrity; however, opportunities exist to ensure the framework more strongly defines and communicates:

- management's zero tolerance towards fraud in order to convey a strong tone from the top
- FRM roles and responsibilities of all key stakeholders
- how the agency defines and monitors its FRM performance
- the importance of employees' role in support of FRM

The agency's FRA is a critical part of its FRM activities; however, there are gaps in the process that must be addressed in order to ensure that responsibilities and accountabilities for owning risks are clear and that fraud risks are proactively and thoroughly identified, assessed and managed.

All these elements, if strengthened, will help ensure that the agency has a FRM approach that is cohesive, integrated across all business areas and, most importantly, effective.

[10] International Public Sector Fraud Forum guidance, Guide to understanding the total impact of fraud

Key findings

An FRM policy or framework, documents an organization's approach to addressing fraud. In 2024, the agency replaced its Internal Fraud Management Framework with a new Integrity Framework. This is important as integrity is essential to supporting a strong culture of values and ethics that helps prevent fraud and sets the organizational tone. However, there are opportunities to better define the CBSA's FRM approach within the framework, including roles, responsibilities, governance, oversight, monitoring and reporting and steps to continuously improve its FRM activities.

An FRA is a critical element of the fraud risk program, as it identifies and determines an organization's exposure to various fraud risks and schemes and the actions to mitigate these risks. Although the agency does conduct FRM activities, there were gaps identified in the approach related to:

- a lack of an extensive FRA over time
- inconsistent consideration of compliance reviews and other corporate documents to inform assessments of risks and controls
- insufficient guidance provided to risk owners who provide information on controls
- lack of a clear definition of roles, responsibilities and accountabilities for risk owners
- insufficient validation and challenge of information on controls

Summary of recommendations

The audit makes two recommendations to support the improvement of the agency's FRM activities which include:

1. Updating the Integrity Framework to further:
    - define the roles and responsibilities and accountabilities of CBSA's stakeholders in FRM and oversight
    - define and document steps to monitor and report on FRM activities, including conflicts of interest, all of the fraud prevention and values and ethics training, and use the information for continuous improvement
2. Updating the risk assessment process to:
    - further define when and how the FRA should be conducted
    - update guidance provided to stakeholders to support the identification of fraud controls
    - clarify roles and responsibilities for risk owners
    - consistently validate the controls included for each risk

Management response

The Canada Border Services agency welcomes the results of the Audit of Fraud Risk Management and accepts all recommendations made.

The CBSA's FRM program continues to build on a strong foundation of financial controls, compliance monitoring, awareness activities, audit and investigations. In the last year, the agency has implemented steps to improve FRM and controls to better mitigate fraud risks, including:

- a new Recourse, Standards and Program Integrity Branch to support all activities and business lines with a compliance lens
- a mandatory self-assessment tool that requires all employees to annually confirm they are aware of their obligations under the CBSA Code of Conduct and the Directive on Conflict of Interest
- a requirement that employees disclose interactions with vendors
- an Executive Procurement Review Committee to ensure senior oversight of the agency's procurement activities

Contributing to broader Government-wide FRM, Public Services and Procurement Canada implemented CBSA's proposed improvement to the Phoenix pay system allowing departments to monitor and review higher-risk pay transactions entered into Phoenix by users with the compensation advisor role.

Through this audit, the CBSA is taking steps to further improve its Integrity Framework, assessment of fraud risks, and identification of fraud controls.

The CBSA is confident that the present action plan in response to the audit's recommendations relating to framework and process will further strengthen the agency FRM program.

Audit findings

The audit resulted in the findings below.

Governing fraud risk management

Summary: We expected that the agency had developed a framework and governance structure with defined roles and responsibilities to support its FRM program. We found that the agency replaced its dedicated FRM framework with an Integrity Framework. Although essential, there are opportunities to further define the agency's approach to FRM by including all roles, responsibilities, accountabilities and oversight to support better integration and coordination of FRM activities.

CBSA's fraud risk management framework

Documenting the elements of an FRM program is an important step to support its governance, implementation and coordination, by setting the expectations of senior management, and employees[11]. It also sets the overall program objectives and requirements.

The audit reviewed the agency's FRM framework to determine whether it included the key FRM elements including defined governance, processes to support conducting a risk assessment, managing fraud controls, monitoring and continuous improvement. To assess the framework, the audit relied on industry best practices from the Committee of Sponsoring Organisations of the Treadway Commission[12]

[11] 2023 COSO Fraud Risk Management Guide

[12] The Committee of Sponsoring Organizations' (COSO) mission is to help organizations improve performance by developing thought leadership that enhances internal control, risk management, governance and fraud deterrence. About Us | COSO

(COSO) as well as the Office of the Auditor General of Canada's published guide for managing its fraud risks[13].

In September 2024, the agency finalized its Integrity Framework (thereafter called "the Framework"), which replaced the 2022 Internal Fraud Management Framework. The new Framework takes a broader view of integrity and looks to integrate and balance human elements with risk processes and controls. Integrity is important as it facilitates a strong culture of values and ethics[14] that helps prevent the commission of fraud in the first place and encourages those who see fraud to report it. However, there are opportunities to better define the agency's specific FRM approach within the framework. Having a clear anti-fraud approach ensures that all key stakeholders understand their roles and responsibilities, reinforces accountability, and supports discussions and decisions on the allocation of anti fraud resources.

Setting the tone from the top

As noted above, fraud can be perpetrated by parties internal or external to an organization. The agency's Framework includes a definition of fraud which focuses on acts that can be perpetrated by employees[15] and does not explicitly make references to external parties within its scope. Defining the specific scope and/or listing the scope exclusions can further clarify the focus of FRM efforts in the agency and can help bring awareness to employees of what should be reported. In addition, a best practice would be to include in the framework a statement regarding the agency's zero tolerance for fraud, reinforcing a strong tone from the top, as well as a statement that no reprisal and retaliation will be taken towards those who do report[16].

Roles and responsibilities

The Framework lists the roles and responsibilities for many key stakeholders, but it does not include all important FRM players. For example, the framework lists the Chief Security Officer as responsible for overseeing the Integrity Program; however, it could more fully reflect FRM oversight by defining the Executive Committee's responsibilities such as approving or endorsing the framework, ensuring sufficient FRM resources and overseeing the performance of the FRM. In addition, the Departmental Audit Committee, who provide objective advice to the Deputy Head on risk management processes, could be added to the Framework to reflect this important and independent role. Documenting all key responsibilities, including FRM oversight, ensures everyone knows their role and can carry it out effectively.

[13] Guide on Managing Risks at the Office of the Auditor General

[14] COSO Fraud Risk Management Guide, "The organization demonstrates a commitment to integrity and ethical values".

[15] CBSA's Integrity Framework, "Intentional act committed to secure and unfair or unlawful gain as well as the deliberate violation of laws regulation and policies by Agency employees (even when the benefit is non financial)".

[16] Managing the Business Risk of Fraud, 2012 Institute of Internal Auditors, Reporting Procedures and Whistleblower Protection

Communicating the fraud risk management approach

The new Integrity Framework was circulated for consultation across various business areas of the agency including the Executive Committee (EC), all regions, branches as well as to the responsible parties identified in the Framework.

However, at the time of the audit, the final Framework, which was approved in September 2024, had not yet been shared with all employees, and a communication plan had not yet been developed. Limited communication of the framework is a missed opportunity to continually reinforce management's zero tolerance stance on fraud, and to increase employee awareness, of their roles and responsibilities towards FRM.

Fraud risk management oversight

Effective FRM starts with a governance structure that addresses fraud risks within their respective governance and oversight responsibilities. The audit reviewed the 2022 and 2024 fraud related frameworks, the terms of reference of agency committees, as well as records of decisions and other governance documents to determine whether a governance structure with defined roles and responsibilities was established to oversee FRM and related control activities. In practice, the:

1. Executive Committee (EC) – President level - reviews and approves the FRP
2. Director General Steering Committee - Director General level - reviews the FRP
3. Integrity Management Working Group (IMWG) – Director level- broadly supports the FRM program and is not a decision making body
4. Departmental Audit Committee receives the FRP for information

None of the four bodies had FRM explicitly stated in their terms of reference, however the terms of reference for the EC, Director General Steering Committee and the Audit Committee all included some responsibility for general risk management such as identifying key risks. Within the audit period, records of decisions for all of the above Committees including the IMWG show that fraud was discussed within the context of the FRP; however, the IMWG had not met for over a year (since May 2023).

The IMWG's mandate is to support the implementation of integrity management activities and its terms of reference lists monitoring activities as one of its responsibilities; however, it is unclear what these specific monitoring activities are. For example, despite increasing concerns around the integrity of agency procurement in January 2023, records of decision do not reflect discussions related to procurement controls that would have benefited from additional monitoring or potential escalation to senior management. This is important because this group is the only dedicated body within the agency with a role to support FRM. Lack of clear roles and responsibilities can limit the proactive management of FRM.

Further, there were no representatives of the regions or the Office of Values and Ethics in this group's membership. This is vital as both the regions and the values and ethics office are considered key stakeholders in FRM: the regions as first line of defence in the implementation of fraud controls and the values and ethics office who manages the agency's Code of Conduct (such as ensuring it is up to date and aligned with policy directives) and the conflict of interest disclosure process. The absence of key stakeholders membership such as the regions and values and ethics office can limit FRM issues from being identified and addressed in a timely manner.

Monitoring fraud risk management

According to the Treasury Board of Canada Secretariat's (TBS) Guide to Integrated Risk Management, monitoring and periodic reviews of the risk management approach and process are essential to ensure the effectiveness, efficiency, and relevance in supporting the organization's overall performance[17].

Similarly, FRM activities should be monitored to determine whether they are functioning as intended and sufficiently managing the agency's risks. The monitoring approach is expected to be documented in a FRM policy or framework and cover details such as the specific performance criteria to be measured, the frequency of monitoring, the stakeholders responsible for providing performance data and those who should be receiving the results, and how the information will be used.

The audit reviewed the 2022 Internal Fraud Management Framework as well as the new Integrity Framework to determine whether expectations for monitoring and reporting the FRM program had been defined. Both the 2022 Internal Fraud Management Framework and the 2024 Integrity Framework included a requirement for the Professional Integrity Division to periodically review the framework.

The new Integrity Framework includes an objective to measure the Framework's performance by reviewing reports and statistics that could identify issues and trends impacting integrity; trends such as misconduct allegations, disclosures of wrongdoing and results from values and ethics-related questions in the Public Service Employee Survey. These are important activities to reflect on, however they could be further strengthened with the introduction and analysis of FRM performance criteria[18] and targets such as, but not limited to:

- establishment of service standards and compliance with identified targets such as the time taken to respond to conflict of interest disclosures[19]
- the agency's compliance with the mandatory conflict of interest affirmations and whether compliance was achieved in the targeted timeframe
- length of time for detecting fraudulent activity and extent of the loss[20]
- anti-fraud communication and promotional activities across the agency[21], such as the number/frequency of messages supporting ethical behaviour delivered to employees by executives[22]
- completion rates of all mandatory fraud and/or values and ethics related training[23]

[17] TBS Guide to Integrated Risk Management, Section 7, Monitoring and Review of the Approach and Process

[18] TBS Guide to Integrated Risk Management, Section 7, Monitoring and Review of the Approach and Process

[19] Guide on Managing Fraud Risks at the Office of the Auditor General of Canada, Annex B, Monitoring Work Plan for the Internal Specialist for Fraud

[20] COSO FRM Guide Establishes Appropriate Measurement Criteria

[21] Guide on Managing Fraud Risks at the Office of the Auditor General of Canada, Annex C2: Fraud Prevention and Detection Scorecard, D28

[22] Ibid.

[23] Ibid.

Recommendation 1

The Vice-President of the Recourse, Professional Standards Branch should update the Integrity Framework to better define the agency's FRM approach, key roles and responsibilities and monitoring of FRM. To support awareness of FRM, the updated framework should be communicated to all agency employees and the results of FRM performance should be periodically communicated to senior management.

Management response: Agreed. The Vice-President of the Recourse, Standards and Program Integrity Branch will update the Integrity Framework to include the agency's approach to identify, assess, mitigate, monitor, and respond to fraud risks. Defining FRM roles and responsibilities will strengthen accountability and collaboration. Communicating the updated framework to employees will increase awareness and support a culture of integrity. Additionally, periodically reporting performance to senior management will provide insights into emerging risks, control effectiveness, and areas for improvement.

Completion date: March 2026

Assessing fraud risks

Summary: We expected that the agency had an adequate process in place to assess and mitigate its internal fraud risks and identify and implement effective fraud controls. The audit found that the agency had a process in place to assess its fraud risks; however, there were gaps in the process which if left unaddressed can lead to poor identification and assessment of risks and controls.

The Fraud Risk Assessment

The FRA is one of the critical elements in an effective FRM program[24]. This is because the FRA identifies the potential fraud-related risks and events that could impact an organization's objectives and its reputation. According to the TBS Integrated Risk Management Framework, this is based on a combination of quantitative and qualitative analysis[25] used to help determine how much the organization is exposed to its risk as well as how much of that risk it is willing to tolerate. At its core, an FRA supports business planning and decision-making in determining which risks should be prioritized, and the allocation of resources to mitigate the fraud risks with the greatest impact.

At the CBSA, the Enterprise Planning Risk and Results Division is responsible for conducting the FRA and documenting the results in an FRP. The FRP is an overview of the key risk information and is an output of the FRA[26]. It is used to communicate risk information to management and support their decision making.

A risk is an event with the potential to affect the achievement of an organization's objectives expressed by the likelihood it could occur and the impact it could have[27].

[24] COSO Fraud Risk Management Guide, "The organization performs a comprehensive fraud risk assessment to identify specific fraud schemes and risks and assess their likelihood and significance, evaluate existing fraud control activities and implement actions to mitigate residual risk."

[25] TBS Framework for the Management of Risk

[26] TBS Guide to Corporate Risk Profiles, The Corporate Risk Profile

[27] TBS Guide to Integrated Risk Management

Frequency of the fraud risk assessment

There is no set frequency for conducting an FRA; however, best practices include assessing and reassessing fraud risks when there are changes to business operations, the external environment, leadership, or when new fraud risks and schemes have emerged[28]. The agency does update the FRP every two years; however, a more formal or extensive risk assessment was last conducted in 2018. At that time, over 40 participants from across the agency were canvassed, through structured interviews and a survey, for their perspective on the internal fraud risks in their respective functional areas. This led to a voting exercise where ten key risks were identified and their exposure ratings (likelihood and impact) were calculated.

The FRP was updated in 2021 and 2023; however, the process was less formal. As it was determined that the agency's risks were stable, no risk interviews were conducted. In 2021, a control rating exercise was conducted to gain perceptions of the importance of controls; however, this exercise focused on four of the previously identified fraud risks. This exercise was not continued in 2023, with no documented rationale for the change in process.

Since 2018, the agency has experienced significant changes to its operating environment including:

- a global pandemic which impacted operations
  - the pandemic also resulted in an increase in loss as a result of fraud worldwide[29]
- the conduct of two simultaneous multimillion dollar transformation initiatives[30]
- a nationalization of internal services (such as human resources)
- changes in key leadership positions

There were no specific criteria to determine when a more formal FRA (such as recalculation of likelihood and impact ratings and agency engagement through risk interviews/surveys) should be conducted despite some of these changes. A lack of defined factors to trigger an extensive risk assessment may lead to missed opportunities to engage key areas of the agency, identify new fraud risks, and respond to changes in exposure to existing fraud risks and schemes.

Identifying fraud risks

The process to identify new risks and schemes can include: consulting with individuals of varying levels of management across the organization, identifying and reviewing information on controls and their effectiveness, conducting environmental scans by reviewing corporate documents that outline strategic and operational plans and objectives, and where possible assessing data analytics, audits and other compliance exercises[31].

[28] COSO Fraud Risk Management Guide, "performs reassessments and assesses changes to fraud risk"

[29] 2024 ACFE Report to the Nations

[30] The CBSA Assessment and Revenue Management (CARM) is the new official system of record for the collection of duties and taxes for commercial good entering Canada and the Traveller Modernization Initiative which will introduce new digital tools to support the processing of travellers.

[31] COSO Fraud Risk Management Guide, "Involves appropriate levels of management" and Guide to Integrated Risk Management - Canada.ca

The audit reviewed the agency’s methodology for identifying new fraud risks and schemes and found that since 2018, the primary approach to identifying fraud risks was through analysis of founded cases of misconduct and some data analytics. Both are good sources of information for identifying new risks or changes to the exposure of current risks; however, there was a missed opportunity to integrate other available information such as risk assessments performed at the regional, branch and enterprise level.

For example, the agency’s Information Science and Technology Branch and the Enterprise Risk Profile had identified the risk that “IT assets could be compromised by external or internal factors” as high, while the FRP includes a risk that “staff may intentionally access, modify, delete, steal, and/or share electronic information assets for non-legitimate purposes…”[32] with a medium exposure. Both risks share similar elements such as risk drivers (internal systems not subject to security checks[33]) and impacts (compromised information, border integrity and delivery of services[34]). The 2021 and 2023 FRPs did not define the scale for the ratings, or the likelihood the risk could occur and the impact it could have. Defining this would allow for a clearer understanding of why this risk would be considered as having a medium exposure while the other two risk assessments considered it high.

In addition, there was no step in the 2023 FRP process where stakeholders were explicitly asked whether they had identified any new fraud risks in their functional areas. A lack of review of other agency risks assessments, clearly defined scale for assessing each risk, as well as explicitly asking about new fraud risks may limit the ability to compile a cohesive, consistent and integrated view of the agency’s existing and emerging fraud risks.

Risk of overriding controls

According to the 2024 ACFE’s Report to the Nations, 19% of fraud cases occur due to an override of controls. Management’s ability to override or circumvent an existing fraud control can render it ineffective. This issue is currently not reflected in the FRP. This is especially relevant to segregation of duties which refers to the general principle that no one individual has complete control over a business process to avoid fraud or misuse of information.

> According to the ACFE, the following were the main control weaknesses contributing to fraud worldwide in 2024[35]:
>
> - 32% Lack of Internal Controls
> - 19% Override of Existing Controls

[32] The full risk statement based on the 2023 FRP, “Staff may intentionally access, modify, delete, steal, and/or share electronic information assets for non-legitimate purposes which may lead to the loss of confidentiality, integrity or availability of the asset(s).”

[33] 2023 FRP Risk Driver for Risk 1 Misuse/Theft of Information “The existence of over 130 internal systems resulting in data integrity issues sometimes developed by local initiatives and never having been subjected to adequate security checks” and ISTB 2023-2024 Branch Risk Profile, Risk 3 IT Security and Cyber Threats, Risk Driver “Local Applications have frequently been developed and implemented lacking IT Security controls or standard development methodology”

[34] 2023 FRP Risk Driver for Risk 1 Misuse/Theft of Information “Compromised border integrity and loss of overall public and industry confidence and trust in the Agency's ability to effectively manage border control” and the ISTB 2023-2024 Branch Risk Profile, Risk 3 IT Security and Cyber Threats “Loss of CBSA information, individuals and assets, as well as the trusted delivery of programs and services”

[35] 2024 ACFE Report to the Nations

- 18% Lack of management review
- 9% Lack of competent personnel in oversight roles
- 8% Poor tone at the top
- 5% Lack of independent audits
- 3% Lack of employee fraud education
- 1% Lack of clear lines of authority
- 1% Lack of reporting mechanism

Internal audits conducted in 2021[36] and 2023[37] identified gaps in system controls, specifically regarding the segregation of duties[38] (although in both audits fraud was not apparent). Additionally, fraud cases perpetrated by individuals at higher levels of management, although less frequent than those by employees, take longer to detect and can lead to greater losses[39]. Lack of consideration of this issue as well as the results of compliance exercises that assess these controls may limit the ability to identify areas where this risk may be present or has increased.

Fraud risks and schemes

A fraud scheme can be a more specific type of fraudulent activity within a risk. For example, bid rigging and fictitious billing can be considered types of schemes that are associated with the broader risk of corruption and asset misappropriation. FRAs are to capture fraud risks, schemes and the controls in place to mitigate each of them. The agency's FRP does capture the major risks; however, it does not capture the related fraud schemes to which the agency may be exposed.

For example, the fraud risk related to contracting and procurement includes the risk that staff may circumvent policies/procedures and/or legislation and award, amend or extend contracts inappropriately. However, the risk information does not capture the many common schemes that can occur in the contracting and procurement space, such as processing duplicate payments intentionally, improper billing, fictitious invoices and phantom vendors. Lack of awareness of these schemes may impact the understanding of the risks the agency is exposed to, hinder employees from identifying and reporting them when they occur and most importantly prevent management from designing specific controls to address them.

Assessing and prioritizing the agency's fraud risks

A standard practice in assessing risk includes determining the likelihood the risk could occur and, if it did occur, the impact it could have on an organization's objectives[40]. This analysis coupled with discussions with management on their risk tolerance (the level of risk they are willing to accept) helps to identify how risks should be prioritized/ranked. The audit reviewed the methodology for assessing and

[36] 2021 Audit of compensation processes and controls: Findings

[37] 2024 Audit of contracting and procurement, 4. Segregation of Duties (SoD)

[38] 2012, IIA Managing the Business Risk of Fraud, "Fraud Risk Assessments should consider the potential override of controls by management as well as other areas where controls are weak or there is a lack of segregation of duties"

[39] 2024 ACFE Report to the Nations

[40] TBS Guide to Integrated Risk Management 4.2 Understanding the Organization and its Context

prioritizing fraud risks and found that the agency last formally calculated the likelihood and impact for each risk in 2018.

Since then, the FRP team determines the trend direction (whether a risk has gone up or down) based on whether founded fraud cases have gone up or down, and whether controls have been added since the last FRP. Not identifying the likelihood and impact of the risk limits management's ability to know which element of the risk may have changed since the last assessment. For example, if the likelihood of a risk remains the same but the potential impact increases (e.g. increased reputational risk due to high media attention and scrutiny from external oversight bodies), management may decide that the risk must be mitigated.

The FRP's assessment of the risks does factor whether controls have been added; however, prior to 2024 it did not reflect available information on control effectiveness/gaps from audits and other compliance reviews such as the Internal Controls for Financial Reporting. For example, following the completion of the risk assessment, the 2023 FRP (presented to Director General Steering Committee in November 2023) identified the agency's exposure to the risk of contracting and procurement as low, despite a March 2023 internal audit that highlighted gaps in the controls and processes with retaining sufficient documentation to demonstrate compliance with contracting policy requirements[41]. That audit finding, the high media attention (as early as January 2023) and the potential increased impact on reputational risk would have been important considerations for updating this risk. As of 2024, results of audits have been reflected in the FRP.

A lack of consistent review of audits and compliance exercises, can lead to the misidentification of the residual fraud risk. In addition, documenting the quantitative analysis for the risk also increases transparency and the ability to both repeat and validate the initial assessment of each risk[42].

Fraud controls

The effectiveness of fraud controls requires an assessment of whether the control is in place and functioning and whether it is effective at preventing and detecting fraud[43]. The audit non randomly selected four of the highest rated fraud risks in the FRP to gather information on the controls listed in the fraud risk sheets, including whether they were operating and were being assessed. These four risks were:

- Risk 1: Misuse/Theft of information
- Risk 2: Theft of physical assets
- Risk 7: Fraudulent reporting of leave and overtime
- Risk 8: Illegally facilitated border crossing (people and goods)

The risk of contracting and procurement was one of the top four risks; however, the audit excluded it from this list as it was recently reviewed in the 2024 Internal Audit of Contracting and Procurement.

[41] 2023 CBSA Internal audit of federal government consulting contracts awarded to McKinsey & Company, "reported poor documentation to support the bid evaluations and section 34 sign off."

[42] TBS Guide to Integrated Risk Management, Risk Management Process, "the risk management process can be thought of as a series of inter-connected and inter-related steps that are repeatable and verifiable."

[43] COSO Fraud Risk Management Guide, Identified Existing Fraud Control Activities and Assesses Their Effectiveness

Validating fraud controls

To update the FRP, a Director level is tasked with providing updated information on the risk, such as updates to the controls and changes to the risk drivers. The information provided is inputted directly into the FRP and is not validated and/or approved by the individual risk owner at the Vice President level, nor is it challenged by the FRP team.

For example, two of the four risks in the FRP included mitigating controls that were not yet in place or not fully implemented. [redacted]. This is important because relying on control activities that are not yet operational can lead the agency to assess its risk exposure lower than it should.

Roles and responsibilities

According to the CBSA's *Risk Management Handbook*, risk owners are defined as having individual or organizational accountability and authority to manage an identified risk. In some cases, there may be multiple risk owners with responsibility for a risk.

All risks in the FRP had identified risk owners, however for two of the four risks, risk owners were not aware of their roles and responsibilities for the breadth of control activities listed, who they belonged to or what their status was. [redacted] however risk leads had no knowledge of who this activity belonged to or what the status of this activity was.

This is because the information that is collected to update the FRP does not link the control activity to its business process owner. A lack of overall accountability around risks and their identified controls could result in poor management of controls which in turn could heighten fraud risks.

Guidance to key stakeholders

Instructions are given to risk leads to provide guidance on the types of information that should be included to update the FRP. These instructions are also supplemented with meetings to help verbally guide the risk leads; however, the audit found that there were opportunities to strengthen the guidance provided to risk leads. For example, the instructions do not include a definition of fraud nor that the focus is on internal fraud. In addition, risk leads are not required to provide information on the purpose of the controls they list, whether they are preventive or detective or what specific fraud element the controls are meant to mitigate.

[redacted][44]; however, neither risk owner knew the details of this control, such as what type of detection technology was being introduced, who were the full-time equivalents, who was responsible for this control and what specific issue this control was meant to mitigate. Lack of clear guidance can lead to the identification of controls that do not address the risk or a misunderstanding of the areas where controls need to be implemented and enhanced.

[44] Full-time equivalents (FTE)

Fraud prevention and values and ethics training

Training (in addition to ongoing communication and supporting tools) is an important preventive fraud control. It can be used to educate and/or remind employees about fraud, their ethical obligations, including disclosing conflicts of interest and providing awareness of insider threats. Mandatory training also supports a strong tone from the top[45]. The audit examined six mandatory values and ethics and fraud prevention related training courses that are required for employees and managers to complete. (refer to Appendix C, Fraud related training). This information was used to determine the level of completion within the audit period April 1 2024 and September 2024 and whether training completion was being monitored and reported on.

Three of the six training courses for employees, Security Awareness, Values, Ethics and Disclosure of Wrongdoing, and Insider Threat had high completion rates at 90%, 89% and 83% respectively. All three of these training courses were being tracked monthly by the Human Resources Branch. However, only two, Security Awareness and Insider Threat, were being reported annually in the Security and Emergency Management Programs Annual Report.

The other three training courses had much lower completion rates and were not consistently monitored and reported on. For example, 57% completed the Values and Ethics Foundations for Employees course. This course is mandatory for new public service employees. The completion is low, however this rate may not reflect the actual training completion rate. This is because there is a possibility that employees took this training in their previous department and that completion was not captured in agency data. In order to see an employee’s full training history, new employees must update their training profile on the Government of Canada’s training platform and indicate CBSA as their new employer. Human Resources Branch confirmed that this may not occur consistently. This is important because the agency may not have accurate information on an important fraud control.

For the two required training courses for managers, Values and Ethics for Managers (mandatory for first-time managers) and Public Servants Disclosure Protection Act (required for all CBSA managers and executives), it was not possible to determine completion rates with an audit level of assurance because the agency does not track the dates when existing employees move into a new manager position.

This means that it is not possible to accurately determine whether all the managers that should have taken the courses, within the given period, did in fact take it. For the audit’s scope period, 53 managers completed the Public Servants Disclosure Protection Act and 74 completed the Values and Ethics for Managers. Based on approximate data as of September 2024, of the roughly 2,000 managers and supervisors at the CBSA, this roughly represents that:

- 2.7% had completed the Public Servants Disclosure Protection Act
- 3.7 % had completed the Values and Ethics for Managers

Neither of these trainings were being monitored and reported on; however, during the course of the audit, the Senior Officer for the Internal Disclosure confirmed that the Public Servants Disclosure Protection Act training would be monitored quarterly. In addition, although the new Integrity Framework includes the Values and Ethics Foundations for Employees training course as a resource and

[45] Guide on Managing Fraud Risks at the Office of the Auditor General of Canada, section 3.1 Fraud Prevention

awareness tool, it did not include the Values and Ethics Foundations for Managers. This is important because according to ACFE, managers or direct supervisors are the most common way that whistleblowers report fraud when a hotline mechanism is not used[46]. They also support in establishing a strong tone at the top by setting examples that promote values and ethics. Lack of awareness and completion of these trainings may limit their ability to carry out their role.

Responding to and monitoring the agency's fraud risks

Once risks have been identified and assessed, the FRP includes a proposed response to each risk such as whether to maintain or strengthen controls, a supporting rationale for each response and in some cases a recommendation when warranted. These responses are presented to EC for discussion and approval. Based on a review of the 2021 and 2023 FRP, all risks included a response and a supporting rationale.

Once EC approves the responses and recommendations, risk owners then develop action plans to address the risks that require further strengthening or any recommendations that have been put forward. The action plans are later developed by the risk owners and also approved by EC.

After EC's approval of the recommendations, risk owners are then responsible for developing action plans; however, risk owners are not consistently involved in the development of the recommendations. Early involvement of risk owners would be beneficial as they can identify upfront resource constraints or other limitations that may impact the way the agency can respond to a risk[47]. This early identification of constraints can support informed decision making, transparency and accountability[48].

The ongoing monitoring of risks is essential to ensuring that risk information remains relevant[49]. There was monitoring of the FRP recommendations with status updates initially provided to EC annually and in 2024, updates increased to quarterly. Although there was regular monitoring, changes to recommendations were not consistently documented.

The 2021 FRP included five approved recommendations. As a follow up, the 2023 FRP included a status update which showed that two of the five were considered complete while three were partially complete. In the following May 2024 quarterly FRP update, one of the partially completed recommendations related to taking steps to manage leave/overtime was not carried forward (and was no longer being monitored), with no documented rationale, approval for the change, or alternative approaches to address the risk.

Recommendations that are not implemented and without documented rationale may indicate that identified gaps in control activities have not been addressed and that fraud risks are not mitigated.

The 2023 FRP included two new recommendations which, at the time of the audit, actions to address them were being implemented.

[46] 2024 ACFE Report to the Nations

[47] TBS Guide to Integrated Risk Management, Risk Response

[48] TBS Guide to Integrated Risk Management, section 6.1 Ongoing Integrated Risk Management

[49] TBS Guide to Integrated Risk Management, Risk Monitoring

Certifying the fraud risk profile

The FRA is not supported by a fraud specialist such as a certified fraud examiner, nor is it certified by an executive to confirm its adequacy[50]. While neither of these are requirements, an important principle is that management consider the skills and experience needed to conduct risk management activities[51].

At the CBSA, some individuals conducting the FRA have received fraud-related training; however, specialized training and certification would provide additional support and expertise in the management of fraud risks, such as providing advice to business areas in their identification and assessment of fraud controls. This can help overall to develop the maturity of the agency's FRM processes.

Recommendation 2

To support the continuous improvement of the FRA and identification of fraud controls, the Vice-President of the Finance and Corporate Management Branch should review and update its FRA process to:

1. further define when and how the FRA will be completed
2. update the FRP guidance provided to risk owners and stakeholders
3. review and update the list of controls for all risks in the FRP to ensure that they are all relevant for mitigating fraud and operating as intended

Management response: Agreed. The Vice-President of the Finance and Corporate Management Branch will conduct a comprehensive update and review of the FRP in 2025 to 2026. This process will identify and reassess current risks and established controls and the monitoring and reporting process and frequency, as well as providing updated guidance to risk owners and stakeholders in reviewing fraud risks and associated controls.

Completion date: April 2026

[50] Guide on Managing Fraud Risks at the Office of the Auditor General of Canada, Annex C. Annual Certification of the Adequacy of the Office's Fraud Risk Assessment

[51] TBS Guide to Integrated Risk Management, section 4.5 Resources

Appendix A: Audit criteria

Lines of enquiry	Audit criteria
1. Fraud Risk Governance: The agency has established, communicated and oversees a Fraud Risk Management Program.	1.1 The agency has developed and communicated to key stakeholders a fraud risk management framework that includes the key elements of effective fraud risk management. 1.2 The agency has established and implemented a governance structure with defined mandates, roles and responsibilities to oversee fraud risk management and related control activities.
2. Fraud Risk Assessment: The agency has an adequate process in place to assess and mitigate its internal fraud risks.	2.1 The agency has established a process to regularly identify, assess, respond to, monitor and report on fraud risks.
3. Fraud Controls (preventive and detective): The agency has a process to ensure it adequately identifies and implements effective controls to prevent and detect fraud.	3.1 The agency has established a process to identify and assess the effectiveness of preventive and detective fraud risk controls.
4. Fraud Risk Monitoring and Reporting: The agency monitors and continually improves its fraud risk management program.	4.1 The agency has a process in place to continuously monitor and report on fraud risk management activities, including values and ethics. 4.2 The agency uses the information from its fraud risk management activities to continually improve its fraud risk management program.

Appendix B: Previous audits

A number of audits in the last five years have highlighted gaps in the controls of key agency processes such as contracting and procurement, payroll, internal controls for financial reporting and border management (people and goods) that are relevant to fraud risk management.

Audit	Findings and recommendations
2024 Audit of ArriveCan (External Audit)	Poor documentation, financial records, and controls around the management of contracts undermined transparency and restricted opportunities for competition. Three recommendations were made to address these serious issues.
2024 Audit of contracting and procurement (Internal Audit)	There were gaps in internal controls such as vulnerabilities in the access to the agency's Corporate Administrative Systems, segregation of duties and lack of proactive monitoring of fraud. Two recommendations were made to address this including proactive monitoring of fraud risks, review of system access and segregation of duties.
2023 Audit of internal control over financial reporting (Internal Audit)	A risk assessment of internal controls was last conducted in 2019. The audit included a recommendation to conduct a comprehensive risk assessment and integrate the risk of fraud.
2021 Audit of compensation processes and controls (Internal Audit)	There were significant issues concerning the internal controls for the HR-to-Pay process including more than half of the controls were not designed, documented, and or operating effectively and incompatible roles (related to segregation of duties) were present and not monitored. Two of the audit's recommendations addresses these issues including ensuring the internal control framework reflected testing of operating effectiveness and monitoring users with incompatible roles.
2019 CBSA, Audit of Revenue Collected by the CBSA (Internal Audit)	There was a need to carry out periodic reviews of user access to revenue collection systems to ensure appropriate access and adequate segregation of duties. The audit includes one recommendation that addresses periodic reviews of user access.
2017 Preventing Corruption in Immigration and Border Services (External Audit)	The agency had not implemented controls to address the risk of corruption at the border. The audit included a recommendation that the agency assess its corruption mitigation controls.

Appendix C: Fraud related training

Table 1: Completion results for employees' values and ethics/fraud-related training between April 1, 2021 and September 2024

Fraud training course	Completion requirement	Completion results	Responsible area	Monitored and reported on
Security Awareness	All employees as soon as possible	90% of new employees between	Security and Professional Standards	Yes
Values, Ethics and Disclosure of Wrongdoing at the CBSA	All employees within 3 months	89% of new employees between	Office of Values and Ethics	Training completion is monitored, but not reported
Values and Ethics Foundations for Employees	All new employees new to the public service within 6 months	57% of new employees between	Office of Values and Ethics	No
Values and Ethics Foundations for Managers	All new managers within 6 months of appointment	Could not assess completion rate n = 74 employees	Office of Values and Ethics	No
Public Servants Disclosure Protection Act	All supervisors, managers and above within 6 months of appointment.	Could not assess completion rate n = 53 employees	Senior Officer of Internal Disclosure	No As of November 2024, training completion will be reviewed quarterly.
Insider Threat	All employees within 12 months	83% of new employees between	Security and Professional Standards	Yes

Appendix D: Glossary

Bribe	Money or favour given or promised in order to influence the judgement or conduct of a person in a position of trust
Controls	A set of measures or actions taken to manage risks and increase the likelihood that established objectives will be achieved
Founded (cases)	To bring something into existence; in the context of the report, identifying fraud cases that has materialized
Fraud	Any intentional act by one or more individuals among employees, management, those charged with governance (internal) or third parties (external) involving the use of deception to obtain an unjust or illegal advantage
Fraud Scheme	A systematic plan/arrangement created to execute a criminal or fraudulent scenario, in order to obtain the personal benefits from it
Impact	Extent to which a risk event might affect the enterprise
Inherent Risk	The level of risk to achieve an entity's objectives and before actions are taken to alter the risk's impact or likelihood
Likelihood	Possibility of a potential risk occurring, interpreted using qualitative values such as low, medium, or high
Residual Risk	Risk that remains after controls to identify and eliminate some or all types of risks have been made
Risk	It is the expression of the likelihood and impact of an event with the potential to affect the achievement of an organization's objectives
Risk Exposure	A measure of possible future loss which my result from an activity or occurrence
Risk Tolerance	The willingness of an organization to accept or reject a given level of residual risk (exposure)
Risk Trend	The direction in which an inherent risk or a residual risk is moving

Appendix E: Acronyms

ACFE	Association of Certified Fraud Examiners
CBSA	Canada Border Services Agency
COSO	Committee of Sponsoring Organisations of the Treadway Commission
EC	Executive Committee
FRA	Fraud Risk Assessment
FRM	Fraud Risk Management
FRP	Fraud Risk Profile
IMWG	Integrity Management Working Group
TBS	Treasury Board of Canada Secretariat