



Environment and
Climate Change Canada

Environnement et
Changement climatique Canada



Fraud Risk Assessment and Governance Review

Summary Report

The Audit and Evaluation Branch
In collaboration with Deloitte LLP

December 2015

Canada 

List of Acronyms

ACFE	Association of Certified Fraud Examiners
AEB	Audit and Evaluation Branch
CAE	Chief Audit Executive
COSO	Committee of Sponsoring Organizations
EAAC	External Audit Advisory Committee
EMC	Executive Management Committee
ECCC	Environment and Climate Change Canada
EFT	Electronic Fund Transfer
FRA	Fraud Risk Assessment
IIA	Institute of Internal Auditors
PIC	Policy on Internal Control
WIP	Work in Progress

Prepared by the Audit and Evaluation Branch

Acknowledgments

The review was done in collaboration with Deloitte LLP and was led by Jean-Luc Tétreault, Audit Manager, under the direction of Stella Line Cousineau, would like to thank those individuals who contributed to this project and, more particularly, the employees who provided insights and comments.

Version Control

File Name:	Fraud Risk Assessment and Governance Review.docx
Date:	December 16, 2015

TABLE OF CONTENTS

EXECUTIVE SUMMARY	1
1. INTRODUCTION AND BACKGROUND	3
2 OBJECTIVES, SCOPE AND METHODOLOGY	3
3 FINDINGS AND RECOMMENDATIONS	5
3.1 Fraud Governance and Management Framework	5
3.2 Fraud Risk Assessment	7
4 CONCLUSION	8
Annex 1 Definitions and Detailed Methodology	9
Annex 2 High and Medium Risk Scenarios.....	12

EXECUTIVE SUMMARY

The *Internal Auditing Standards for the Government of Canada*¹ require internal audit to evaluate the potential for the occurrence of fraud and how the organization manages fraud risk. Treasury Board guidance² further clarifies the need for the Chief Audit Executive (CAE) to contribute to the reduction in fraud risk by ensuring that adequate fraud risk management strategies are in place to discourage the commission of fraud to minimize losses should it occur.

As such, this review was included in the departmental 2013 Risk-Based Audit and Evaluation Plan as approved by the Deputy Minister, upon recommendation of the External Audit Advisory Committee (EAAC). Deloitte LLP (Deloitte) was retained by the Audit and Evaluation Branch (AEB) to conduct this review. This project had two distinct objectives. The first one included an assessment of the governance and management framework regarding the prevention, detection, investigation, response and reporting of fraud and fraud related events. The second one, the conduct of a high level Fraud Risk Assessment (FRA) of the organization. The five elements of the COSO³ framework were used to assess the governance and management framework of the Department.

Given the possible sensitivity of the information contained in Deloitte's report pertaining to both the review and the FRA, AEB is presenting through the following report, a summary of Deloitte's findings⁴ and AEB's consolidation of the recommendations.

With respect to the assessment of the fraud governance and management framework, Deloitte has determined that overall Environment and Climate Change Canada (ECCC) has designed and implemented many policies and procedures which are, for the most part aligned with the COSO framework leading practices. However, some shortfalls exist in the areas of governance and policy.

In addition, Deloitte has identified a number of areas for improvement in the context of the FRA along with suggestions to reduce the risk of fraud. Given that these suggestions still need to be confirmed and reviewed by management, the detailed results were provided separately to responsible Branch Heads.

Recommendation 1

With the support of the Deputy Minister and in consultation with the Executive Management Committee members, Corporate Services Branch should coordinate the review of the governance and policy framework over the management of fraud, in order to clarify the roles and responsibilities and to enhance the existing policies to address the observations raised by Deloitte.

¹ Government of Canada has adopted the *Institute of Internal Auditors (IIA) International Professional Practices Framework*

² *Responsibilities and Accountability of Internal Audit for the detection, Investigation, and Reporting of Possible Fraud*

³ COSO – Committee of Sponsoring Organizations of the Treadway Commission's, "Internal Control – Integrated Framework"

⁴ Assessment of the governance and management of the fraud framework and the completion of a fraud risk assessment – Environment and Climate Change Canada, Deloitte LLP, February 2015

Management Response

Agree. Corporate Services Branch will review the mandate and terms of reference of the Departmental Security Committee and ECCC Policy on the Conduct of Administrative Investigations.

Recommendation 2

The Assistant Deputy Minister from Finance Branch, Corporate Services Branch, Human Resources Branch, Enforcement Branch and Environmental Stewardship Branch should review the detailed observations and suggestions presented in Deloitte's report and ascertain whether the suggested actions for improvement should be implemented.

Management Response

The Assistant Deputy Ministers from Finance Branch, Corporate Services Branch, Human Resources Branch, Enforcement Branch and Environmental Stewardship Branch agrees with the recommendation. The detailed management responses can be found under Section 3 of this report.

1. INTRODUCTION AND BACKGROUND

This review was included in the 2013 Integrated Departmental Risk-Based Audit and Evaluation Plan as approved by the Deputy Minister, upon recommendation of the External Audit Advisory Committee (EAAC).

Good governance principles demand that an organization’s board of directors, or equivalent oversight body, ensure overall high ethical behaviour in the organization, regardless of its status as public, private, government, or not-for-profit; its relative size; or its industry. Vigilant handling of fraud cases within an organization sends clear signals to the public, stakeholders, employees and regulators about senior management’s tolerance toward fraud risks⁵.

In today's environment with increased legislative and regulatory requirements, there is a greater need for organizations to understand and address fraud risks. The likelihood of fraud occurring can be reduced by implementing effective antifraud programs and controls that can minimize any resulting damage. Fraud prevention and detection also makes good business sense and can provide cost savings to organizations, in addition to reduce other harmful consequences.

The *Internal Auditing Standards for the Government of Canada* require internal audit to periodically evaluate the potential for the occurrence of fraud and how the organization manages fraud risk. Treasury Board guidance further clarifies the need for the CAE to contribute to the reduction in fraud risk by ensuring that adequate fraud risk management strategies are in place to discourage the commission of fraud to minimize losses should it occur.

Deloitte LLP (“Deloitte”) was retained by the AEB to review the governance and management framework regarding the prevention, detection, investigation, response and reporting of fraud and fraud related events, and to conduct a high level fraud risk assessment of the organization.

This assessment was conducted using a methodology consistent with the COSO framework as described in the Deloitte white paper titled, “*Anti-fraud Programs and Controls*”, dated 2004, as well as other recent pronouncements⁶ by international accounting bodies.

2 OBJECTIVES, SCOPE AND METHODOLOGY

Objectives

The objectives of this project were to:

- review the fraud governance and management framework regarding the prevention, detection, investigation, response and reporting of fraud; and
- conduct a high level Fraud Risk Assessment (FRA).

⁵ Managing the Business Risk of Fraud – A Practical Guide Sponsored by the Institute of Internal Auditors, The American Institute of Certified Public Accountants and the Association of Fraud Examiners

⁶ Consideration of Fraud in a Financial Statement Audit (Statement of Auditing Standards 99 – October 2002).

The objectives, scope and approach for the project were presented at Executive management Committee (EMC) and EAAC in June 2014. The results of the FRA were also presented at the March 2015 EAAC meeting. A summary of the FRA results is provided in Section 3.2 of this report.

Scope - Fraud Risk Assessment

The business components included in the scope of the FRA specifically included:

- Procurement / Expenditure / Payables;
- Capital Assets / Assets Under Construction;
- Inventories;
- Revenues/ Accounts Receivable;
- Intangible Assets/ Confidential or Classified Information; and
- Human Resources/Payroll.

These business components were not intended to be all inclusive and were selected based on the documentation review conducted by Deloitte. These business components also aligned with most government departments, thus providing the basis for some comparison.

Scope - Governance Review

In the context of this Fraud Governance Review, the following components derived from the COSO Framework were considered:

1. Creating a Control Environment (Fraud Risk Governance);
2. Performing Fraud Risk Assessments;
3. Designing and Implementing Antifraud Control Activities;
4. Sharing Information and Communication; and
5. Monitoring

Methodology

Deloitte has conducted the FRA through a documentation review, a series of interviews and brainstorm sessions with a broad spectrum of Environment and Climate Change Canada (ECCC) managers and employees from different branches. The fraud scenarios identified in the context of this FRA were mapped against ECCC's internal control to assess whether the mapped controls would either prevent or detect the scenario, thereby reducing the likelihood of a scenario occurring, and determine the overall residual risk for each scenario.

Given the possible sensitivity of the information contained in Deloitte's report pertaining to both the review and the FRA, this report presents a summary of Deloitte's findings and the AEB's consolidations of the recommendations. Deloitte's more detailed report and findings were provided separately to responsible Branch Heads.

In addition, the results from Deloitte's report⁷ will be reviewed further by the AEB and will be further considered as part of its annual audit planning exercises as well as during the planning of individual audit projects conducted in related areas.

The detailed methodology is provided in Annex 1 of this report.

Statement of Conformance

The review portion of this project conforms to the *Internal Auditing Standards for the Government of Canada*, as supported by the results of the quality assurance and improvement program, and as applied in the context of a review.

In our professional judgement, sufficient and appropriate audit procedures have been conducted and evidence gathered to provide reasonable assurance on the accuracy of the conclusions reached and contained in the review portion of this report. However, testing of the controls was not performed. The conclusions were based on a comparison of the situations as they existed at the end of the fieldwork in December 2014.

3 FINDINGS AND RECOMMENDATIONS

3.1 Fraud Governance and Management Framework

Deloitte has determined that ECCC has effectively designed and implemented many policies and procedures which are, for the most part aligned with the COSO framework leading practices. For example, the existence of ECCC Values and Ethics Code of Conduct, the existence of an Administrative Investigation Policy as well as ECCC Internal Control Framework and Monitoring Strategy for Internal Control Management. However, gaps still exist in some areas. The following presents the AEB's summary of Deloitte's findings.

Role and Responsibilities

While there is a policy on the Conduct of Administrative Investigation and a Departmental Security Committee in place, the role and responsibilities over the governance and management of fraud and the coordination of fraud allegations are not entirely clear.

The review noted that information regarding fraud cases is not being shared and communicated to all relevant stakeholders in a systematic manner. As well, the AEB has noted that the current Departmental Security Committee does not directly address fraud risks or cases.

Also, the current Administrative Investigation Policy does not explicitly identify Finance Branch (FB) as a supporting office related to fraud. In many instances, FB can identify relevant information as it pertains to Fraud Investigation, in addition to playing a key role in the design of appropriate controls to mitigate the Fraud risks. Not involving all relevant stakeholders in the process increases the risk that control activities that may have failed

⁷ Assessment of the governance and management of the fraud framework and the completion of a fraud risk assessment – Environment and Climate Change Canada, Deloitte LLP, February 2015

may not be effectively addressed and/or reviewed by the appropriate business line. In addition, there is a risk that this information is not adequately considered in the context of departmental risk planning.

Policy

ECCC does not have a formal departmental fraud policy. While some components of a corporate fraud policy are covered through various means (policy on the Conduct of Administrative Investigation, the Internal Control Framework, Values and Ethics Code of Conduct, Learner's Roadmaps, and the Monitoring Strategy for Internal Control Management), some gaps remain.

In reviewing ECCC's policy on the Conduct of Administrative Investigation, Deloitte noted that the current policy could be improved in the following areas:

- use of outside counsel of specialist when required;
- formal guidance regarding the potential for conflict of interest during the investigative process;
- vacation monitoring;
- fraud training for new hires and periodic training for all employees;
- ethical behaviour expectation of vendors;
- tracking/logging of fraud cases;
- periodic update of the FRA; and
- tracking the performance of antifraud efforts.

A more integrated fraud policy/strategy would help ensure that fraud is addressed in a comprehensive and integrated manner. The fraud policy should also include a definition of fraud, responsibility structure for managing fraud, organizational attitude to fraud, policy on disciplinary action and identification of a central function and individual as a responsible party for the anti-fraud programs and controls program. The goal of a corporate fraud policy is to safeguard the reputation and financial viability of an entity through improved management of fraud risk.

Recommendation 1

With the support of the Deputy Minister and in consultation with the Executive Management Committee members, Corporate Services Branch should coordinate the review of the governance and policy framework over the management of fraud, in order to clarify the roles and responsibilities and to enhance the existing policies to address the observations raised by Deloitte.

Management Response

Agree. Corporate Services Branch will review the mandate and terms of reference of the Departmental Security Committee and ECCC Policy on the Conduct of Administrative Investigations.

3.2 Fraud Risk Assessment

Deloitte has identified and validated potential fraud risk scenarios relevant to the business components identified in the scope section of this report. This was achieved through a documentation review, a series of interviews and brainstorm workshops. The scenarios were mapped to ECCC’s internal controls to assess whether the controls would either prevent or detect the scenario, and determine the overall residual risk for each scenario.

In total, 58 unique fraud scenarios were developed through this process. Of these unique fraud scenarios, 19 were assessed as having medium or high residual risk. The table below depicts the results for the 58 identified risk ranked scenarios by business components.

This table also shows the comparison to other public sector organizations results. While ECCC’s business components show a slightly higher percentage of residual risk, Deloitte has indicated that ECCC is well within the acceptable range.

Risk Scenarios by Business Components

	# of scenarios	Inherent Risk Assessment (before consideration of controls)			Residual Risk Assessment (after consideration of controls)		
		High	Medium	Low	High	Medium	Low
Billing or Payment Scheme	3	0	1	2	0	1	2
Corruption – COI, Bribery, Bid Rigging	13	3	7	3	1	7	5
Fraudulent Financial Reporting	3	0	2	1	0	0	3
Misappropriation of Assets	31	3	13	15	1	8	22
Misrepresentation / Conflict of Interest	3	0	1	2	0	0	3
Payroll Scheme	5	0	2	3	0	1	4
Total	58	6	26	26	2	17	39
Percentage of Total	100%	10%	45%	45%	3%	29%	67%
Other Public Sector Organizations	100%	17%	40%	43%	2%	23%	76%

Note: The category of “Other Public Organizations” is based on an average of 11 Public Sector Fraud Risk Assessments recently completed by Deloitte and is intended to provide guidance on EC’s performance relative to others within the Public Sector. Deloitte did not assess the comparability of these other Public Sector organizations to EC for the purposes of comparing the nature and extent of fraud risks.

Deloitte presented under a separate report the results of the FRA along with the suggested remedial actions or improvements to existing controls for high and medium residual risk scenarios. The information contained in the detailed report was provided to responsible Branch Heads under separate cover.

Recommendation 2

The Assistant Deputy Minister from Finance Branch, Corporate Services Branch, Human Resources Branch, Enforcement Branch and Environmental Stewardship Branch should review the detailed observations and suggestions presented in Deloitte’s report and ascertain whether the suggested actions for improvement should be implemented.

Management Response

Finance Branch, Corporate Services Branch, Human Resources Branch, Enforcement Branch and Environmental Stewardship Branch accepts the recommendation to analyze the detailed observations outlined in Deloitte's report to determine the extent to which suggested actions can be implemented.

4 CONCLUSION

AEB has determined that ECCC has designed and implemented many policies and procedures which are, for the most part, aligned with the COSO framework leading practices. However, potential shortfalls and areas for improvements exist in the areas of fraud governance and policy. In addition, a number of potential areas of improvement in the context of the FRA along with suggestions to reduce the risk of fraud were identified.

Annex 1

Definitions and Detailed Methodology

A- Fraud definitions

For the purposes of the fraud risk assessment and review, the following fraud definitions were used to assist in defining fraud:

The Criminal Code S. 380(1)

“Everybody who, by deceit, falsehood or other fraudulent means, whether or not it is false pretence within the meaning of this Act, defrauds the public or any person, whether ascertained or not, of any property, money or valuable security or service”.

According to the Chartered Professional Accountants of Canada

“The term fraud refers to an intentional act by one or more individuals among management, other employees, those charged with governance, or third parties, involving the use of deception to obtain an unjust or illegal advantage”.

According to the Institute of Internal Auditors

“Any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage.”

B- Fraud Governance Review Methodology

The following key COSO Framework components of a Fraud Management Framework were used in the context of this review:

- **Creating a Control Environment (Fraud Risk Governance)** – “Tone at the Top” – attitude of the senior management team towards the overall risk and control environment regarding managing unethical behavior. Culture of the organization in relation to resistance to fraud, corruption and other unethical behavior.
- **Fraud Risk Assessment** - Analysis of external and internal fraud risks that could negatively impact the achievement of the Organization’s strategic objectives.
- **Designing and Implementing Antifraud Control Activities** - Controls established throughout the Organization to prevent and detect the risk of fraud and corruption.
- **Sharing Information and Communication** regarding antifraud and anticorruption program activities.
- **Monitoring Activities** both in respect of antifraud and anticorruption program and controls measures and initiatives to help ensure that the system remains effective and dynamic.

Professional judgment was applied when evaluating the design of the antifraud programs and controls, because the nature and extent of an effective antifraud program

will vary from entity to entity. The nature and extent of an effective antifraud program depends on a number of factors, including the nature of the business, the number of locations, and the results of the entity's Fraud Risk Assessment. To assess ECCC's current state, we compared ECCC's current Program and control initiatives, policies and procedures with:

1. COSO Internal Control – Integrated Framework;
2. American Institute of Certified Public Accountants (“AICPA”) Managing the Business Risk of Fraud; and
3. Accepted leading practices that organizations with mature programs have found to be better practices.

Deloitte's procedures involved identifying and analysing the present inventory of antifraud and related policies and activities existing within ECCC. These initiatives, policies and elements were then compared with leading practices within each of the five COSO framework areas listed above.

This approach was designed to provide ECCC with an indication of where it is at present and the gaps to be considered to achieve with the COSO framework and other relevant standards that reflect leading practices.

C- Fraud Risk Assessment Methodology

The fraud risk assessment was completed in a four phase process as follow:

1. Identified fraud risk factors relevant to ECCC through a series of interviews with ECCC management and employees and developed fraud risk scenarios.
2. Conducted brainstorm workshops with management and employees to:
 - a. validate the fraud risk scenarios,
 - b. identify additional fraud risk scenarios relevant to ECCC,
 - c. risk rank fraud risk scenarios as to likelihood (on an inherent basis, without the consideration of existing controls) and significance, and
 - d. determine the overall inherent risk rating for each scenario based on an equal weighting of likelihood and significance.
3. Conducted a gap analysis of the organization's internal controls to:
 - a. identify and map ECCC's internal controls (from internal control process documentation and through interviews with management and employees) that mitigate the Medium and High inherent fraud risk scenarios,
 - b. compare, where possible, ECCC's controls to expected controls found in similar (Public Sector) organizations,
 - c. assess whether the mapped controls would either prevent or detect the scenario, thereby reducing the likelihood of a scenario occurring, and
 - d. determine the overall residual risk for each scenario.
4. Developed recommendations to address the risk scenarios that were determined to have a level of residual risk at Medium and High.

In total, 58 unique fraud risk scenarios were developed through the fraud risk assessment process. Some of the 58 unique scenarios were presented to multiple

groups in order to obtain different perspectives on the scenarios, resulting in duplication of some of the scenarios from group to group.

The controls mapped to scenarios as part of this assessment include controls that were identified as process-level controls in accordance with the objectives of the financial reporting requirements of Policy on Internal Control (PIC), as well as other controls found in the process narratives and other ECCC documentation that were not specifically identified and documented as controls.

In addition to the above documentation, Deloitte also identified additional undocumented antifraud controls based on follow-up interviews and correspondence with ECCC management and employees during the validation exercise. The residual risk ranking was assessed based on the assumption that internal controls were operating as documented/described as no testing of internal controls was done.

In addition to the process-level controls that have been mapped to the fraud scenarios as detailed above, ECCC has also implemented entity-level controls as part of their overall risk-mitigation strategy. The entity-level controls have been specifically mapped to scenarios when deemed appropriate.

While Deloitte has identified and mapped various ECCC controls that could deter and/or detect each of the fraud risk scenarios; they have not performed any additional testing of these controls. Therefore, Deloitte is unable to confirm that the identified controls are, in fact, effectively mitigating each fraud risk scenario

Project Key Dates

Opening conference (launch memo)	December 2013
Approach and methodology presented to EMC	May 2014
Approach and methodology presented to EAAC	June 2014
Review plan completed	July 2014
EAAC tabling of the Fraud Risk Assessment	March 2015
EMC tabling of final report for information	June 2015
EAAC tabling of final report	June 2015
Deputy Minister approval	December 2015

Annex 2 High and Medium Risk Scenarios

The following section provides a listing of the high and medium residual risk scenarios.

#	Business Components and Processes	Scenario Description
Misappropriation of Assets		
1	Human Resources and Payroll/ Finance/ Procurement	An employee provides confidential information for personal gain in exchange for a personal benefit.
Corruption – Conflict of Interest, Bribery, Bid Rigging		
2	Intangible Assets and Confidential or Classified Information/ Program Areas	An employee uses "insider" knowledge for personal gain.
Misappropriation of Assets		
3	Financial Reporting, Revenues and Accounts Receivable Procurement and Expenditures	Supplier in collusion with an employee submits an invoice for goods or services not provided, or at inflated amounts by a supplier.
4	Financial Reporting, Revenues and Accounts Receivable Capital Assets, Assets Under Construction and Inventories	Writing-off or classification of inventory as obsolete and then takes or sells the inventory for personal gain.
5	Financial Reporting, Revenues and Accounts Receivable	Credit and/or refund to fictitious customer or to a personal account
6	Financial Reporting, Revenues and Accounts Receivable Intangible Assets and Confidential or Classified Information	Credit and/or refund for permit to a party while still providing the permit in order to obtain a kickback or other personal benefit
7	Procurement and Expenditures	Changes to the vendor master file by setting-up fictitious vendors or modifying information for existing vendor to personally receive payments on valid or fictitious invoices.
8	Procurement and Expenditures Capital Assets, Assets Under Construction and Inventories	A supplier is awarded a contract based on certain requirements, and then substitutes for cheaper goods (e.g. Real Property construction contracts, Work in Progress assets).
9	Procurement and Expenditures	A contractor provides multiple bids by submitting phantom bids from shell companies (i.e. either to have multiple bids considered, and/or to have the appearance of a competitive process).
10	Human Resources and Payroll	Frequent unauthorized absenteeism from the workplace. Failing to report days off.
Billing or Payment Scheme		
11	Procurement and Expenditures	Electronic funds transfer (EFT) - diversion of outgoing funds by altering bank account or other information to benefit a third party or for personal gain.
Corruption – Conflict of Interest, Bribery, Bid Rigging		

#	Business Components and Processes	Scenario Description
12	Procurement and Expenditures	A supplier falsifies qualifications, certifications and/or assurances and is awarded contract for services (e.g., construction contract).
13	Procurement and Expenditures	Contractors collude to manipulate the competitive procurement process (either through bid rotation scheme, bid suppression scheme etc.).
14	Procurement and Expenditures Capital Assets, Assets Under Construction and Inventories	Use of multiple sole-source contracts to the same contractor in order to obtain a kickback or other personal benefit.
15	Procurement and Expenditures Capital Assets, Assets Under Construction and Inventories	Agreements are made between an employee and a supplier to award a contract based on lower requirements, and then increase the price through amendments once the contract has been awarded, in order to obtain a kickback or other personal benefit.
16	Intangible Assets and Confidential or Classified Information	An employee fails to take action on an entity that do not fully and/or accurately comply with rules and regulations, in exchange for a personal benefit.
17	Intangible Assets and Confidential or Classified Information	Commercial entities inappropriately influence employees/ management with respect to the setting of rules and/or regulations.
18	Intangible Assets and Confidential or Classified Information	An employee is in a conflict of interest situation with regards to an entity with respect to compliance and/or enforcement activities
Payroll Scheme		
19	Human Resources and Payroll	An employee colludes with manager and submits timesheet for fictitious hours worked.