



**Justice Canada**

**Audit of the Monitoring of the  
System of Internal Control Over  
Financial Reporting**

*Audit Report presented to the  
Departmental Audit Committee  
October 2015*

Internal Audit Services

*Approved by the Deputy Minister at the  
Departmental Audit Committee Meeting on  
October 7, 2015*

Information contained in this publication or product may be reproduced, in part or in whole, and by any means, for personal or public non-commercial purposes, without charge or further permission, unless otherwise specified.

You are asked to:

exercise due diligence in ensuring the accuracy of the materials reproduced;

indicate both the complete title of the materials reproduced, as well as the author organization; and

indicate that the reproduction is a copy of an official work that is published by the Government of Canada and that the reproduction has not been produced in affiliation with, or with the endorsement of the Government of Canada.

Commercial reproduction and distribution is prohibited except with written permission from the Department of Justice Canada. For more information, please contact the Department of Justice Canada at: [www.justice.gc.ca](http://www.justice.gc.ca).

©Her Majesty the Queen in Right of Canada,  
represented by the Minister of Justice and Attorney General of Canada, 2015

ISBN 978-0-660-03740-0

Cat. No. J2-417/2015E-PDF

## Table of Contents

1. Executive Summary.....	1
Introduction.....	1
Strengths .....	1
Areas for Improvement.....	2
Audit Conclusion and Opinion .....	2
Management Response .....	2
2. Statement of Conformance .....	3
3. Acknowledgement.....	3
4. Background.....	4
5. Audit Objective.....	6
6. Audit Scope .....	6
7. Audit Approach .....	7
8. Findings, Recommendations and Management Action Plan.....	7
8.1 Governance.....	8
8.2 Identifying key accounts, processes and sub-processes, risks and key controls .....	11
8.3 Planning and conducting assessments.....	16
8.4 Action plans and remediating control weaknesses.....	21
9. Audit Opinion .....	22
Appendix A – Audit Criteria.....	23

# 1. Executive Summary

## Introduction

The Treasury Board *Policy on Internal Control (PIC)* states that Parliament and Canadians expect the federal government to be well managed with the prudent stewardship of public funds, the safeguarding of public assets, and the effective, efficient and economical use of public resources. It further states that Parliament and Canadians expect reliable reporting that provides transparency and accountability for how government spends public funds to achieve results for Canadians.

The *PIC*, which came into effect on April 1, 2009, requires that Deputy Ministers and Chief Financial Officers sign an annual Statement of Management Responsibility Including Internal Control Over Financial Reporting (Statement). This Statement prefaces a department's annual financial statements and acknowledges management's responsibility for maintaining an effective system of internal control over financial reporting (ICFR). In support of the Statement, the *PIC* requires that departments conduct an annual risk-based assessment of the system of ICFR to determine its ongoing effectiveness. The results of this assessment are reported in a separate annex to the financial statements.

Departments move through three stages of a maturity model to achieve compliance with *PIC*; the design effectiveness stage, the operating effectiveness stage, and the ongoing monitoring stage. The Department of Justice Canada (the Department) is in the ongoing monitoring stage.

Monitoring the ongoing effectiveness of the system of ICFR is essential in ensuring that control weaknesses that might potentially impact the reliability of financial information are identified and corrected.

The Financial Policy and Controls Division (FPCD) within the Finance and Planning Branch (FPB) is responsible for planning and conducting the annual risk-based assessment of the system of ICFR and preparing the annex to the annual financial statements.

## Strengths

Justice Canada was among the first departments to enter the ongoing monitoring stage, achieving this milestone on April 1, 2009. This remains a notable accomplishment, as the 2014-15 Management Accountability Framework assessment reported that only 15 of 34 departments have attained this stage.

Other strengths include: an appropriate and effective governance and oversight framework to support the monitoring of the system of ICFR; the use of multi-year plans and annual results reports; and an effective approach to remediating identified control weaknesses and following up on management action plans.

## **Areas for Improvement**

Opportunities for improvement were noted in the identification of key controls related to financial reporting, and in the risk-based planning and conducting of the annual assessment of the system of ICFR. A more rigorous and better-documented approach to this work will help ensure it is repeatable and that the appropriate key controls are tested to achieve *PIC* objectives.

## **Audit Conclusion and Opinion**

In my opinion, there is room for improvement in the management control framework to monitor the system of ICFR.

An effective governance and oversight is in place, but reporting to oversight bodies should be improved to provide greater level of detail in the testing that is conducted and to better support their decision making. Greater rigour is required in identifying key PLCs, ELC, and ITGCs, and in documenting the risk-based selection of key controls for OE testing each year. Annual OE testing should also be improved to ensure it is sufficient to determine the ongoing effectiveness of the system of ICFR.

Finally, although largely informal, existing processes for reporting and addressing identified control weaknesses appear generally effective and appropriate.

## **Management Response**

Management is in agreement with the audit findings, has accepted the recommendations included in this report, and has developed a management action plan to address them. The management action plan has been integrated in this report.

## 2. Statement of Conformance

In my professional judgment as Chief Audit Executive, the audit conforms to the *Internal Auditing Standards for the Government of Canada*, as supported by the results of the Quality Assurance and Improvement Program.

Submitted by:

*Original signed by*

*October 7, 2015*

---

Inanc Yazar, CPA CGA, CIA, CRMA  
Chief Audit Executive  
Department of Justice Canada

---

Date

## 3. Acknowledgement

The Chief Audit Executive would like to thank the audit team and those individuals who contributed to this engagement and particularly, employees from the Financial Policy and Control Division who provided insights and comments as part of this audit.

## 4. Background

### Treasury Board Policy

The Treasury Board *Policy on Internal Control (PIC)* states that Parliament and Canadians expect the federal government to be well managed with the prudent stewardship of public funds, the safeguarding of public assets, and the effective, efficient and economical use of public resources. It further states that Parliament and Canadians expect reliable reporting that provides transparency and accountability for how government spends public funds to achieve results for Canadians.

The *PIC* came into effect on April 1, 2009, and requires that Deputy Ministers and Chief Financial Officers sign an annual Statement of Management Responsibility Including Internal Control Over Financial Reporting (Statement). The Statement prefaces a department's annual financial statements and acknowledges management's responsibility for maintaining an effective system of internal control over financial reporting (ICFR). In support of the Statement, the *PIC* requires that departments conduct an annual risk-based assessment of the system of ICFR to determine its ongoing effectiveness. The results of this assessment are then reported in a separate annex to the financial statements.

Departments move through three stages of a maturity model to achieve compliance with the *PIC*; the design effectiveness stage, the operating effectiveness stage, and the ongoing monitoring stage. The design effectiveness stage requires that departments identify and document their key controls over financial reporting, and assess whether they are aligned with the risks they aim to mitigate. In the operating effectiveness stage, departments assess the extent to which key controls over financial reporting are operating as intended over a specified period of time, such as a year or six months. Once this first full assessment of ICFR is complete and any identified weaknesses have been remediated, departments move to the ongoing monitoring stage. In this stage, departments conduct periodic, risk-based retesting of key control effectiveness to determine the ongoing effectiveness of the system of ICFR.

While a department may be operating in the ongoing monitoring stage, process and environmental changes may occur and new risks may emerge. To the extent that new risks and key controls to mitigate these new risks are identified, the design and operating effectiveness of these key controls must be assessed as part of the ongoing monitoring stage.

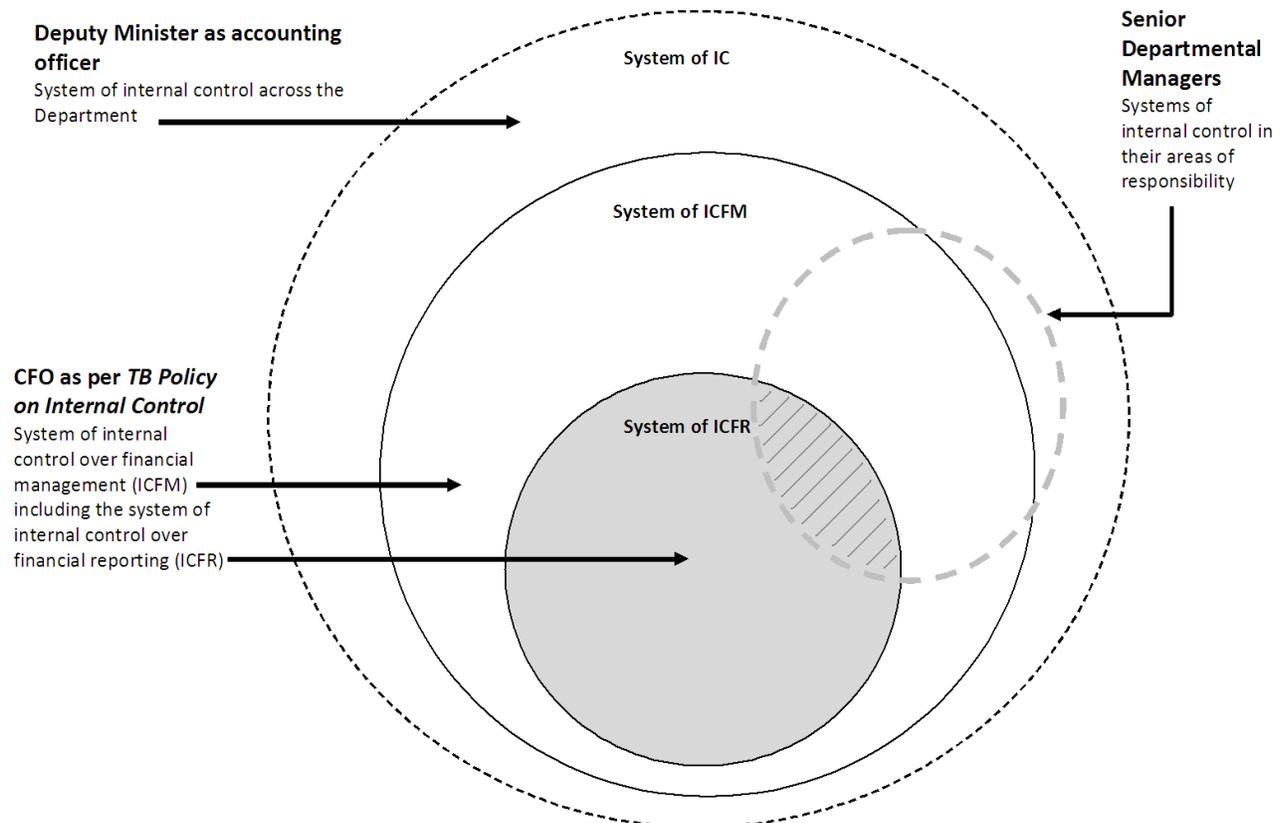
### Internal Controls over Financial Reporting

Internal controls over financial reporting are the procedures and activities put in place by a department to provide reasonable assurance that:

- records which fairly reflect all financial transactions are maintained;
- recording of financial transactions permits the preparation of internal and external financial information, reports, and statements in accordance with policies, directives and standards; and
- revenues received and expenditures made are in accordance with delegated authorities and unauthorized transactions that could have a material effect on financial information and

financial statements are prevented or detected in a timely manner. This includes providing reasonable assurance that financial resources are safeguarded against material loss due to waste, abuse, mismanagement, errors, fraud, omissions and other irregularities.

As illustrated below, a department's system of ICFR is a subset of its system of Internal Controls over Financial Management, which is in turn a subset of its overall system of Internal Controls.



Controls can be categorized into one of three levels: entity level controls (ELCs); information technology general controls (ITGCs); and business process level controls (PLCs).

- **ELCs** are high-level controls that concern the overall operating environment of the department and include tone at the top, ethics, risk management, communications, and human resources.
- **ITGCs** are controls that impact the overall department-wide IT environment, such as access to computer programs and data, program changes, program development and computer operations.
- **PLCs** are those controls embedded in specific business processes used for the processing of specific financial transactions (e.g. account verification, accounts payable, accounts receivable). The effectiveness of these controls is directly and indirectly influenced by the effectiveness of the ELCs.

All three levels of control operate together in an integrated manner to collectively reduce, to an acceptable level, the risk of not achieving an objective.

## **Monitoring of the System of ICFR at Justice Canada**

The Financial Policy and Controls Division (FPCD) within the Finance and Planning Branch (FPB) supports the Department's Assistant Deputy Minister, Management Sector and Chief Financial Officer (ADM/CFO) and the Deputy Chief Financial Officer (DCFO) in discharging their responsibilities for the system of ICFR, including ensuring departmental compliance with the *PIC*. Reporting directly to the DCFO, FPCD plans and conducts the annual risk-based assessment of the system of ICFR and prepares the annex to the annual financial statements.

The Department completed its initial design effectiveness (DE) and operating effectiveness (OE) testing in 2008-09, through an audit readiness project and an Auditor General pilot audit of the 2007-08 financial statements. The Auditor General subsequently issued an unqualified opinion on the 2008-09 financial statements, noting that Justice Canada was the first department to undergo an external audit of their financial statements and congratulating management on its commitment to the initiative. Justice Canada was among the first departments to enter the ongoing monitoring stage, achieving this milestone on April 1, 2009. This remains a notable accomplishment, as only 15 of 34 departments were identified as having attained the ongoing monitoring stage in the 2014-15 Treasury Board Secretariat Management Accountability Framework assessment. In fiscal year 2014-15, the Department completed its first three-year ongoing monitoring program.

Monitoring the ongoing effectiveness of the system of ICFR is essential in ensuring that control weaknesses that might potentially impact the reliability of financial information are identified and corrected.

## **5. Audit Objective**

The objective of the audit was to provide assurance that the management control framework established by FPB to monitor the system of ICFR is adequate and effective.

## **6. Audit Scope**

The audit assessed the monitoring of the ongoing effectiveness of the system of ICFR. This included assessing the risk-based process in place to identify and assess/reassess key controls over financial reporting and address identified control weaknesses. In addition, the audit assessed the governance framework in place to oversee the monitoring of the system of ICFR. The audit did not assess the operating effectiveness of individual ELCs, ITGCs and PLCs.

The audit focused primarily on ICFR assessment activities planned and conducted between 2012-13 and 2014-15.

## 7. Audit Approach

This engagement was conducted in accordance with the Internal Auditing Standards for the Government of Canada and the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing. These standards require that the engagement be planned and performed in such a way as to obtain reasonable assurance that the objectives of the engagement are achieved.

The audit included: structured interviews with FPCD staff, the DCFO and select business process owners (i.e. management and/or staff responsible for specific business processes within Justice Canada); a review of departmental documentation relating to ICFR developed by FPCD and oversight bodies; a review of ICFR-related policies, guidance and documentation developed by Treasury Board, the Office of the Comptroller General, Treasury Board Secretariat *PIC* working groups, other federal government departments, and industry organizations (e.g. COSO, COBIT); and file testing for a sample of ICFR assessments conducted between 2012-13 and 2014-15. This file testing included an in-depth examination of the assessments conducted for ELCs, ITGCs, and three financial statement accounts at the process level (Legal Services Revenue, Capital Assets, and Transfer Payments).

## 8. Findings, Recommendations and Management Action Plan

This section provides the observations and recommendations resulting from the audit work carried out. It is consistent with the lines of enquiry and audit criteria identified in the planning phase and structured as follows:

- Governance;
- Identifying key accounts, processes and sub-processes, risks and key controls;
- Planning and conducting assessments; and
- Action plans and remediating control weaknesses.

## 8.1 Governance

The audit examined whether an effective governance and oversight framework was in place for the monitoring of the ongoing effectiveness of the system of ICFR.

### Finding 1 :

Appropriate and effective oversight bodies are in place to oversee the monitoring of the system of ICFR, however current reporting requires greater detail to support oversight bodies in fulfilling their ICFR related duties.

### Linkage to :

**Governance**

### ICFR Governance Framework

A departmental ICFR Framework, approved by the Deputy Minister in October 2013, is in place and defines ICFR-related roles and responsibilities for key individuals (including executives, senior managers, and employees), committees, offices and divisions within the department. The OCG recently recognized the Department's framework as a "notable practice" – many other departments had not yet developed a formal framework – and the Department agreed to share the framework with other departments.

The primary oversight bodies for ICFR are Management Committee (MC) and the Departmental Audit Committee (DAC). MC is an appropriate oversight body, as Management is responsible for its system of internal controls, including controls over financial reporting, and any identified weaknesses will require management action. DAC also has an important role in ICFR, as they are responsible for recommending the financial statements to the Deputy Head for approval<sup>1</sup> and providing advice to the Deputy Head on the risk-based assessment plans and associated results related to the effectiveness of the departmental system of ICFR<sup>2</sup>.

Our review of meeting minutes from these two committees found that the committees met regularly and addressed ICFR-related matters as required.

### Reporting to Oversight Bodies

Oversight bodies require regular reporting to keep them informed of ICFR monitoring activities and to support them in fulfilling their ICFR-related duties. Every three years, FPCD presents oversight bodies with its On-Going Monitoring Program for ICFR Multi-Year Plan (Multi-Year Plan) for the upcoming three-year period. FPCD also provides formal annual reporting through the:

<sup>1</sup> This requirement is defined in the Statement of Management Responsibility Including Internal Control Over Financial Reporting that precedes the department's financial statements.

<sup>2</sup> As per the Treasury Board *Directive on Internal Audit*, 2012.

- Financial Statement’s Annex – Assessment of Internal Controls Over Financial Reporting (Annex); and
- Results of the On-Going Monitoring Program for ICFR under the Policy on Internal Control report (Results Report).

Throughout the year and as necessary, FPCD also provides ad-hoc reporting on internal controls related to ongoing departmental initiatives (such as the Procure to Pay and Cost Recovery Process Improvement projects).

The Annex is a high-level summary report, presented in a prescribed format defined by the *Guideline for the Policy on Internal Control*. FPCD has recognized that this reporting is not sufficient to support effective oversight, and has developed the Multi-Year Plan and the Results Report to provide greater detail to Management and oversight bodies. This additional reporting is a good practice, but we found it could be improved to more fully support oversight bodies in making informed decisions on the appropriateness and adequacy of ICFR monitoring activities.

The Multi-Year Plan is developed to define the “financial statement accounts to be monitored to ensure ongoing compliance with the *PIC*” over a three-year period. We found this report to provide useful information for oversight bodies, but that greater level of detail is required on FPCD’s approach to determining the ongoing effectiveness of the system of ICFR. The Multi-Year Plan does not explain that the scope of testing to be conducted on identified accounts will be based on a risk assessment conducted at the start of each year and that only select sub-processes and key controls will be tested. Without this information, readers may be left with the expectation that planned testing will include all sub-processes and key controls within the selected accounts. Further, the most recent Multi-Year Plan could have provided more detailed information on the risk scores that were assigned to the accounts (impact, likelihood and overall risk scores), given that risk scores inform the frequency of testing of individual accounts.

The Results Report provides an overview of the results of ICFR monitoring activities conducted in the previous year. The report does not, however, provide sufficient contextual detail for the accounts that were tested, such as the number of sub-processes and controls tested relative to the total number of sub-processes and key controls that exist within the account. Without this broader context, it is difficult for oversight bodies to assess the completeness of testing and to determine if it was sufficient.

The development of a Multi-Year Plan and annual Results Report are strong practices FPCD has implemented in addition to policy requirements. Further refining and improving these documents will better support oversight bodies in making informed decisions on the appropriateness and adequacy of ICFR monitoring activities.

<b>Recommendation 1</b>	<b>Management Action Plan</b>
<p>R-1 It is recommended that the Assistant Deputy Minister Management Sector and Chief Financial Officer improve reporting to oversight bodies to more fully describe the risk-based approach applied in monitoring ICFR, including the scope and extent of operating effectiveness testing that is planned and conducted.</p>	<p>Building on the established process of presenting the annual Internal Controls over Financial Reporting (ICFR) Results Report and other related information (e.g. ICFR Multi-Year Plans) to Management Committee (MC) and the Departmental Audit Committee (DAC) as part of the annual Departmental Financial Statements (DFS) package; the 2015-16 ICFR Results Report will be revised as appropriate, to more fully describe the risk-based approach taken in monitoring ICFR. The ICFR Results Report will be presented to MC and DAC as part of the 2015-16 DFS package by August 31, 2016.</p> <p>The 2015-18 ICFR Multi-Year Plan presented to DAC in June 2015 will be updated as appropriate, to more fully describe the risk-based approach to monitoring ICFR. The updated Plan will cover the period of up to 2016-19 and will be included in the 2015-16 DFS package.</p> <p>As per the established process, feedback regarding the ICFR Results Report and Multi-Year Plan will be requested from MC and the DAC, including the depth of information to be captured, in order to further refine the plans and reports in subsequent years.</p>
<b>Office of Primary Interest :</b>	Assistant Deputy Minister and Chief Financial Officer, Management and CFO Sector
<b>Due Date :</b>	August 31, 2016

## 8.2 Identifying key accounts, processes and sub-processes, risks and key controls

Implementation of the *PIC* requires that key controls be subject to assessment based on risk. A critical first step in this process is identifying and assessing/re-assessing risks and the related key controls that exist within business processes and sub-processes, as well as at the entity level and within IT systems. Properly identifying and assessing risks and related key controls helps ensure effective risk-based decisions on the controls to be monitored each year and helps support the OE testing that is conducted.

### Finding 2 :

Risks and related controls have not been adequately identified and documented to support effective, risk-based ongoing monitoring.

### Linkage to :

Risk management and internal control

### Process Level Controls (PLCs)

In the Department, PLCs are considered and assessed as they exist within financial statement accounts. FPCD records process-level risks and their related controls (PLCs) in “lead sheets” by financial statement account. These lead sheets record the sub-processes, risks and related controls that exist within the account. They also record the risk scores (likelihood, impact and overall) and the characteristics of the PLCs identified (i.e. preventive or detective; automated or manual; financial statement assertion(s) addressed by the control). The recording of risks and key controls, whether in lead sheets or in risk and control matrices, is common across departments and is an essential first step in support of the monitoring of the system of ICFR.

We found that while lead sheets have been established for all three of the financial statement accounts we examined, risks and key controls within identified sub-processes were not always adequately identified and documented. The lists of risks developed by FPCD were in some instances incomplete, and the assessment of identified risks was not always adequate or appropriate (i.e., risks were grouped and scored together, rather than independently; overall risk ratings – high, medium and low – did not always align with likelihood and impact assessment scores). We also found that documented controls were not always well defined and, in some cases, did not address the identified risk. Finally, we noted there were risks for which no controls had been identified.

We also found that all three lead sheets had sub-processes that had not yet been documented. Accordingly, no risks or key controls had been identified. FPCD explained that these sub-processes were deemed low-risk and were therefore not considered for OE testing. We were not able to validate these risk assessments as they were not documented. While we recognize that low risk sub-processes may not require documenting, we noted that four of the sub-processes we identified as missing have been included for OE testing in FPCD’s 2015-16 workplan. In one instance, FPCD added the sub-process to their lead sheet and assessed it as a “medium” risk – a

higher score than was assigned to four of the account's other sub-processes whose risks and controls were previously documented.

These deficiencies do not necessarily imply that FPCD is unaware of the risks or key controls that exist within processes and sub-processes, or that necessary controls do not exist. However, given these deficiencies, we were unable to determine whether FPCD considers all relevant information in developing its risk-based selection of controls for monitoring each year or whether the OE testing it conducts is sufficient to determine the ongoing effectiveness of the system of ICFR (discussed further in sub-section 8.3).

### **Entity Level Controls (ELCs)**

ELCs impact the overall effectiveness of the system of internal controls and can have a fundamental impact on the reliability of controls at the process level if not in place and operating effectively. To identify ELCs, departments select an appropriate benchmark framework<sup>3</sup> to determine relevant control objectives and then identify the specific controls that exist within the department in relation to each of these control objectives. As a point of reference, an OCG-established *PIC* sub-committee on ELCs suggested that there are "approximately 75-100 control objectives to address", while the OCG's 2012 Draft *PIC* Diagnostic Tool for Departments and Agencies (Diagnostic Tool) identified 138 entity level controls.

We found that FPCD's current list of ELCs is not sufficiently complete to support the ongoing monitoring of the system of ICFR. In 2009-10, FPCD identified approximately 200 ELCs for the Department (using the OCG Core Management Controls framework). However, as explained by FPCD, this list was subsequently narrowed, on a risk-basis, to focus on those directly related to financial controls. Currently only 16 ELCs are identified. While we considered FPCD's use of the OCG's Core Management Controls to identify ELCs to be appropriate, we found the current list of ELCs to be deficient. Of the 16 "controls", we considered only five to have been recorded as actual controls. The remaining "controls" represented either control objectives (e.g., "Executive Committee and its Mandate") or a mix of controls and control objectives.

While we agree with FPCD's general approach to identifying key ELCs, it is important that these ELCs be appropriately defined - not just the control objectives. Without a well-defined and complete listing of ELCs, it is not possible to appropriately test the operating effectiveness of ELCs or to conclude on the operating effectiveness of the system of ICFR.

### **Information Technology General Controls (ITGCs)**

ITGCs apply to the components, processes and data of IT systems and include controls around access, operations, and system development and maintenance. Application controls (often considered with ITGCs) are controls embedded in business process applications designed to support outcomes such as authorization, completeness, accuracy and validity of transactions. In general, departments identify ITGCs by first developing risk assessment criteria to document and

---

<sup>3</sup> For example, the COSO (Committee of Sponsoring Organizations of the Treadway Commission) framework, or the OCG Core Management Controls.

assess ICFR-related risks inherent to their IT systems and then identify the specific controls that exist within the systems to mitigate these risks.

We found that FPCD does not currently maintain a list of specific ITGCs. Rather, FPCD has identified a total of five IT “control domains” that support the Department’s IT systems. These IT “control domains” are: systems/data access; security; change controls; program development; and computer operations. Our review noted that while multiple controls would exist within each of these “control domains”, no specific controls have been identified. FPCD explained that, since they don’t have the expertise to identify the relevant ITGCs that exist within the Department’s IT systems, they had intended to leverage two government-wide transformation initiatives to help document the Department’s ITGCs (i.e. Procure to Pay (P2P) and the Financial Management Transformation (FMT) initiatives). However, one of the initiatives was cancelled in December 2013 (P2P) and the other has been delayed (FMT). As a result, limited progress has been made on identifying and documenting ITGCs.

FPCD’s current approach to identifying ITGCs is not sufficient. Even if FPCD had been successful in leveraging these government-wide initiatives to identify certain ITGCs, there remains additional ITGCs that extend beyond the core financial management systems addressed by the initiatives. Of note, in 2007, departmental ITGCs and IT application controls relating to financial reporting were documented. While the list is currently not maintained or used to support ICFR monitoring, it may provide a useful starting point for developing a list of current ITGCs.<sup>4</sup>

Recommendation 2	Management Action Plan
<p>R-2 It is recommended that the Assistant Deputy Minister Management Sector and Chief Financial Officer implement a process to ensure that key controls are appropriately identified, documented and maintained to adequately support ongoing monitoring of the system of ICFR. This will include:</p> <ul style="list-style-type: none"> <li>• Documenting sub-processes, risks and key controls for all in-scope financial statement accounts;</li> </ul>	<p><u>Process Level Controls (PLCs)</u></p> <p>The 2016-19 ICFR Multi-Year Plan (refer to recommendation #1) will include a revised financial statement accounts monitoring schedule, which will change the current annual “breadth-based focus” to a more “in-depth testing focus”. This new monitoring schedule will include less accounts per year but more in-depth testing, providing the same level of assurance overall. Building on the existing monitoring process and documentation, relevant sub-processes of financial statement accounts will be fully documented during the course of the monitoring projects. The documentation of relevant sub-processes, risks and key controls for all in-scope financial statement accounts will be completed throughout the 2016-19 ICFR Multi-Year Plan cycle. Milestones will be completed each year beginning in 2016-17 as accounts are monitored as scheduled, with initial work having already been started in 2015-16.</p>

<sup>4</sup> This audit report refers to ITGCs within those IT systems managed by Justice Canada. For the IT systems managed by other government departments (i.e. Public Works and Government Services and Shared Services Canada), FPDC relies on these OGDs to identify and assess ITGCs within their systems.

- Fully identifying and documenting ELCs and ITGCs; and
- Developing a process to ensure this information is validated and maintained.

A process to ensure the information is validated and maintained going forward will be developed and documented in the Financial Policy and Controls Division (FPCD) ICFR deskbook by August 31, 2016 for PLCs, as well as Entity Level Controls (ELCs) and Information Technology General Controls (ITGCs) as appropriate. The process will be designed so that any new methodologies, direction, etc. from the Office of the Comptroller General can be integrated going forward.

#### Entity Level Controls (ELCs)

The ELCs were fully identified in 2009-10 and updated in 2011-12, with no gaps identified. The ELCs were subsequently grouped and narrowed down to those relevant to ICFR for administrative ease for on-going monitoring.

By March 31, 2016, the ELCs that were grouped will be ungrouped into more specific controls to better identify ELCs that could impact PLCs.

#### Information Technology General Controls (ITGCs)

Recognizing the benefits of documenting ITGCs, significant resources were previously invested in systems projects that were unfortunately cancelled at the direction of the Treasury Board Secretariat (TBS). As a result, moving forward in regards to ITGCs will require consultations with TBS regarding the intention and timeline for new government-wide standard systems via the Financial Management Transformation initiative. The documentation of ITGCs moving forward and deadlines will be based on those consultations to ensure that any ITGC work performed will align with TBS initiatives and will effectively use available resources. For context, ITGCs work going forward will focus on the Integrated Financial and Materiel System (IFMS), as there have been significant changes in the ownership of, and reliance on, other systems since the initial ITGC documentation in 2007. Relevant ITGCs within other Justice Canada managed IT systems will also be assessed, to determine their ICFR-related risks and to determine how they should be monitored going forward.

#### **Office of Primary Interest :**

Assistant Deputy Minister and Chief Financial Officer, Management and CFO Sector

**Due Date :** ELCs

- March 31, 2016

PLCs, ELCs & ITGCs

- August 31, 2016 (Development and documentation of process for validating and maintaining documentation for sub-processes, risks and controls - as appropriate)

PLCs

- March 31, 2019 (with annual milestones, as per the 2016-19 ICFR Multi-Year Plan)

ITGCs

- Subject to TBS direction

### 8.3 Planning and conducting assessments

The on-going monitoring stage of the *PIC* implementation requires departments to conduct an annual risk-based assessment *to determine the ongoing effectiveness* of the system of ICFR. In this regard, departments conduct regular risk assessments to identify and select specific processes and key controls for operating effectiveness testing. OE testing is intended to demonstrate the reliability of controls over a period of time in reducing related financial reporting risks. It requires that testing methodologies and sampling strategies be developed and that sample transactions be selected and tested.

**Finding 3 :**

A more rigorous approach to planning and conducting the annual risk-based assessment of the system of ICFR is required.

**Linkage to :**

Risk management and internal control

#### Process Level Controls (Planning OE Testing)

FPCD's approach to selecting key controls for OE testing begins with the identification of the Department's financial statement accounts for testing. This occurs every three years and, as noted earlier, is documented in FPCD's Multi-Year Plan. The plan also defines the frequency with which the accounts will be tested (i.e., every year; every second year). We found FPCD's approach to identifying financial statement accounts for testing and determining the frequency of their testing to be generally appropriate. In 2011, FPCD conducted a thorough risk assessment that considered information from a number of sources and sought input from senior management. In 2014, FPCD streamlined this process, focusing on whether any significant changes occurred that might influence the previous assessment's results. While this streamlined approach was appropriate for 2014, a more thorough approach to update the 2011 base assessment may be required for future Multi-Year Plans.

On an annual basis, FPCD: 1) re-validates the appropriateness of the financial statement accounts identified for testing in the Multi-Year Plan; and 2) identifies specific sub-processes and key controls within the accounts for testing (as not all sub-processes or key controls within an account are tested). We found FPCD's approach to re-validating the appropriateness of selected accounts to be appropriate, but noted the re-validation was not documented. The re-validation exercise focuses simply on whether any significant changes occurred since the Multi-Year Plan's creation that would influence the account selection. FPCD reported that changes rarely occur that are significant enough to alter the accounts identified for planned testing (e.g., the materiality of accounts do not fluctuate significantly; departmental operational objectives tend to be constant). We did, however, note several weaknesses in the approach employed by FPCD to identify specific sub-processes and key controls within identified accounts for OE testing.

FPCD reported that staff meet annually to consider and select sub-processes and key controls for OE testing. Selection is determined based on the results of previous OE testing and factors such

as recent process changes, the results of recent internal audits and areas of concern to Management. However, this annual risk-based selection is conducted informally and is not documented. Additionally, FPCD's ICFR deskbook provides limited guidance to staff on how to conduct the risk-based selection, nor does it provide a framework for defining the minimum level of testing necessary to allow FPCD to conclude on the ongoing effectiveness of the system of ICFR. By way of example, no requirements have been established for the frequency or extent of testing of high, medium or low risk-related controls. Notably, our review of file testing found that controls related to high risks were not subject to more frequent testing than those related to low or medium risks. Given these weaknesses, we were unable to verify whether the controls identified for testing were the most appropriate or whether the testing would be sufficient to support FPCD's determination of the ongoing effectiveness of the system of ICFR.

While these deficiencies do not necessarily indicate that inappropriate controls are being selected for OE testing, they do increase the likelihood that key risks or controls will be overlooked, or that testing will be insufficient to achieve the objectives of the ongoing monitoring plan. This is of particular concern given that there is no requirement that all key controls within identified financial statement accounts be subject to testing. FPCD's informal planning process is also particularly dependent on staff knowledge and experience, and is therefore vulnerable should a key member of the team leave the group. Finally, as previously noted in subsection 8.2, risks and related controls in processes and sub-processes have not been adequately identified and documented, which may impact FPCD's ability to conduct a fulsome risk assessment.

### **Process Level Controls (Conducting OE Testing)**

As FPCD does not document the results of the risk assessment it conducts each year to select specific sub-processes and key controls for OE testing, we were unable to assess whether OE testing was conducted as planned at the sub-process/key control level. However, we were able to assess whether OE testing was conducted at the financial statement account level as planned, as this information is recorded in FPCD's Multi-Year Plan and in the Annex.

We found that in two of the three years covered by the 2012-2015 Multi-Year Plan, OE testing of financial statement accounts was not completed as planned or as reported in the Annex. In 2012-13, only two of five identified accounts were subject to OE testing, while the Annex reported that OE testing within all five accounts was completed as planned. In 2014-15, only six of seven identified accounts were subject to OE testing (the Annex for this year had not been finalized at the time of our review but the draft we reviewed indicated all testing was completed as planned). FPCD explained that planned OE testing at the account level is sometimes replaced with other activities, such as reviewing and assisting with the design of new controls as a result of process changes.

Most notably, the Legal Services Revenue account was only subject to OE testing in one year over the 3-year period. Further, the testing that was conducted addressed only one of five identified sub-processes in the account. Legal Services Revenue exceeds \$300M annually, representing roughly 25% of the Department's annual revenues and expenses. It is one of only five accounts scheduled for annual OE testing. FPCD explained that while formal OE testing within the account was affected by recurring changes in process design, sufficient testing and

assurance was obtained on the operating effectiveness of key controls within the account based on the design change work performed by FPCD. It was not apparent to us that the work described by FPCD was sufficient to provide assurance on the operating effectiveness of key controls within the account, and we noted that FPCD did not retain records of this testing or report the results in the annual Results Reports or the Annexes (other than to confirm testing had been completed as planned).

While we recognize that process changes can impact scheduled OE testing, OE testing of key controls in relation to high materiality and/or high risk financial statement accounts should be conducted as planned to ensure FPCD is able to conclude on the ongoing effectiveness of related controls. OE testing is rigorous, systematic, and documented, and cannot be replaced by other forms of informal testing. If OE testing as planned is simply not possible during transition periods, the Annex should clearly communicate that processes and key controls were not assessed as planned.

### **Entity Level Controls**

FPCD's approach to assessing the operating effectiveness of ELCs is to monitor, on an annual basis, the results of assessments conducted by others. These assessments include internal audits, the Management Accountability Framework, the Public Service Employee Survey, and relevant OCG and OAG audits. In its deskbook, FPCD explains that in tracking and reporting on the results of assessments conducted by others, FPCD monitors the operating environment of the Department as to whether it would have a negative or positive impact on the processes or controls over financial reporting.

ELCs can be subjective and difficult to measure. We found FPCD's strategy of monitoring the results of assessments conducted by others to be an appropriate approach to assessing ELCs. However, we noted that the assessments that were conducted by others did not always address all relevant ELCs, with no approach having been established by FPCD to address gaps in testing. FPCD's deskbook indicates that performing ELC assessments is "beyond the mandate" of its program. However, the OCG related documentation we reviewed made clear the obligation of departments to conduct OE testing of ELCs.

Weaknesses within ELC can have a fundamental impact on the reliability of controls at the process level. Where reliance is placed on testing conducted by others, assessment gaps need to be identified and addressed. Once ELCs have been adequately defined by FPCD (see sub-section 8.2), an approach should be established for testing, as appropriate, the ELCs not assessed by others.

### **Information Technology General Controls**

Similar to ELCs, FPCD's approach to assessing the operating effectiveness of ITGCs is to monitor, on an annual basis, the results of assessments conducted by others (in this case IT system owners). Further, their deskbook explains that this approach includes FPCD conducting 'monitoring projects' when there are significant gaps in the assessments conducted by others. While FPCD reported the conduct of some limited testing of its own in 2012-13 and 2013-14, its

deskbook acknowledges that they do not have the technical expertise to necessarily conduct ITGC assessments.

We did not find FPCD’s approach to monitoring to be sufficient to allow them to determine the ongoing effectiveness of ITGCs. While relying on the results of assessments conducted by others is a recommended practice, FPCD tracks the results of assessments conducted by others against “control domains” rather than specific ITGCs. As noted in section 8.2, FPCD has not identified specific ITGCs that would allow it to adequately identify gaps in the assessments conducted by others. Further, it is not apparent that the gaps that are identified are being addressed. Our review noted that of the five systems managed by the Department, only two had monitoring results recorded for all five “domains” over the three-year period. One system did not have any assessment results to consider, and two others had assessments that only partially addressed the five “domains”.

As FPCD has not adequately identified the Department’s ITGCs or established an approach for testing ELCs not assessed by others, it is not possible to determine whether OE testing is sufficient to determine the ongoing effectiveness of the system of ICFR. Gaps in the assessments conducted by others must be identified and addressed. This is particularly relevant for ITGCs, as system assessments conducted by others are not necessarily focused on the same objectives as ICFR, and may not address the appropriate controls.

Recommendation 3	Management Action Plan
<p>R-3 It is recommended that the Assistant Deputy Minister Management Sector and Chief Financial Officer develop, document and implement an approach for the annual selection of key controls for OE testing (PLCs, ELCs, and ITGCs). This approach should include:</p> <ul style="list-style-type: none"> <li>• The risk factors to be assessed and how they influence the selection of controls (i.e., weighting);</li> <li>• The minimum level of testing required to determine the ongoing effectiveness of the system of ICFR; and</li> <li>• A process for identifying and addressing gaps where testing by others is not sufficient to</li> </ul>	<p>Within the Government of Canada, there are other policies, directives and reporting requirements in addition to the PIC that require Departments to provide assurance on the accuracy of financial reporting. To meet these additional requirements there are other various types of assurance work performed in addition to Operating Effectiveness (OE) testing.</p> <p><u>Process Level Controls (PLCs)</u></p> <p>In this context, the Management and CFO Sector will provide the DAC with a summary report of the work performed and previously reported to DAC and senior management which provided assurance on financial reporting from 2009-10 to 2014-15 for each financial statement account. The Summary report will demonstrate that an appropriate level of PLCs assurance work has been performed. This summary report will be provided by December 31, 2015.</p> <p>In addition, the FPCD PIC working folders have been updated to provide clearer links to the other attestation, controls design, and policy work performed that provide</p>

<p>assess the selected key controls.</p>	<p>assurance in addition to OE testing. Going forward, FPCD will also maintain records of project files so that evidence regarding assurance work on the design of new processes and controls will be more readily available.</p> <p>Finally, the updating of documentation in the FPCD deskbook and working documents over the 2016-19 ICFR Multi-Year Plan cycle (refer to recommendation #2, work to be completed by March 31, 2019) will include the development of a risk-based approach for selecting sub-processes and controls to be tested and the levels of testing to be conducted in order to provide assurance.</p> <p><u>Entity Level Controls (ELCs)</u></p> <p>Options and a recommendation regarding operating effectiveness testing going forward for ELCs will be provided to the Deputy Minister by January 31, 2016 for approval.</p> <p>The above-noted approach to support the approved option for ELCs will be documented as part of the overall deskbook updates outlined in the management action plan for recommendation #2 by August 31, 2016.</p> <p><u>Information Technology General Controls (ITGCs)</u></p> <p>The ITGCs risk documentation will be developed as part of recommendation #2. Based on the consultations with TBS, an operating effectiveness testing plan will be developed once the ITGCs documentation has been updated and design effectiveness has been re-assessed.</p>
<p><b>Office of Primary Interest :</b></p>	<p>Assistant Deputy Minister and Chief Financial Officer, Management and CFO Sector</p>
<p><b>Due Date :</b></p>	<p><u>PLCs</u></p> <ul style="list-style-type: none"> <li>• December 31, 2015 (Summary report to DAC)</li> <li>• March 31, 2019 (Completion of documentation)</li> </ul> <p><u>ELCs</u></p> <ul style="list-style-type: none"> <li>• January 31, 2016 (Options for operating effectiveness testing provided to the Deputy Minister)</li> <li>• August 31, 2016 (documentation of approach based on DM decision)</li> </ul> <p><u>ITGCs</u></p> <ul style="list-style-type: none"> <li>• Subject to TBS direction</li> </ul>

## 8.4 Action plans and remediating control weaknesses

As ICFR testing is conducted, errors or deficiencies in control design and/or operating effectiveness may be detected. Management must consider the potential impact of any control weaknesses on the integrity of the financial statements and determine if remedial action is required to address the control deficiencies. Therefore, a process should be in place to notify Management of control deficiencies and to monitor any control remediation actions.

FPCD has implemented an informal process for reporting control deficiencies to Management and monitoring the resulting action plans. As FPCD identifies control deficiencies, they are reported to the appropriate functional leads and FPCD works with them to develop an action plan to mitigate the deficiency. FPCD reported that most control deficiencies are resolved within the fiscal year in which they are identified. If the deficiency is not resolved by fiscal year-end, it is noted in the Results Report and the Annex to the financial statements (if warranted). FPCD then monitors implementation of the outstanding item until its completion.

This informal process is supported by two factors that help ensure its success. First, FPCD and the majority of process owners responsible for ICFR reside within the Finance and Planning Branch and report to the DCFO. This provides FPCD with an effective mechanism for addressing any outstanding control deficiencies. Second, the Assistant Deputy Minister and Chief Financial Officer has implemented a process whereby process and control changes within Management and CFO Sector will not be approved until they have been reviewed by FPCD.

Although we expected to find a more formal reporting and follow-up process, we concluded that the existing informal process is effective at this time. We noted that control deficiencies were generally addressed as they were identified, and that outstanding issues were monitored by FPCD and reported to oversight bodies as required.

## 9. Audit Opinion

In my opinion, there is room for improvement in the management control framework to monitor the system of ICFR.

An effective governance and oversight is in place, but reporting to oversight bodies should be improved to provide greater level of detail in the testing that is conducted and to better support their decision making. Greater rigour is required in identifying key PLCs, ELC, and ITGCs, and in documenting the risk-based selection of key controls for OE testing each year. Annual OE testing should also be improved to ensure it is sufficient to determine the ongoing effectiveness of the system of ICFR.

Finally, although largely informal, existing processes for reporting and addressing identified control weaknesses appear generally effective and appropriate.

## Appendix A – Audit Criteria

### Line of Enquiry 1 – Governance Framework

Criterion 1.1 - An effective governance framework is in place to provide oversight over the monitoring of the ongoing effectiveness of the system of ICFR.

### Line of Enquiry 2 – Identification of Key Accounts, Processes and Sub-Processes, Risks and Key Controls

Criterion 2.1 - An adequate and appropriate approach is applied in identifying key accounts of the financial statements for ICFR assessment.

Criterion 2.2 - An adequate and appropriate approach is applied in identifying processes and sub-processes, risks and controls for ICFR assessment.

### Line of Enquiry 3 – Planning and Conducting Assessments

Criterion 3.1 - Sufficient and appropriate plans are developed to support assessment of the ongoing effectiveness of the system of ICFR.

Criterion 3.2 - Sufficient and appropriate activities are conducted to support assessment of the ongoing effectiveness of the system of ICFR.

### Line of Enquiry 4 – Action Plans to Address Control Weaknesses

Criterion 4.1 - Appropriate action plans are developed and implemented to address identified control weaknesses.