Deloitte.

Internal Audit of IM/IT Governance

Office of the Privacy Commissioner of Canada

March 24, 2015
FINAL REPORT

Table of Contents

1. Executive Summary 1

Background and Context 1

Summary of Findings 1

Conclusion 2

Statement of Conformance 2

2. Audit Objective, Scope and Approach 3

Background 3

Audit Objective and Scope 4

Audit Approach 4

3. Findings and Recommendations 6

Strengths Noted 6

Audit Findings 6

Finding #1: IM/IT Strategic Planning 6

Finding #2: Application Oversight and Change Control 9

Finding #3: IM/IT-Enabled Project Management 11

Appendix A – Interviewees 14

Appendix B – Audit Criteria 15

1. Executive Summary

Background and Context

The Office of the Privacy Commissioner of Canada (OPC) is responsible for overseeing compliance with both the *Privacy Act*, which covers the personal information-handling practices of federal government departments and agencies, and the *Personal Information Protection and Electronic Documents Act (PIPEDA)*, Canada's federal private-sector privacy law.

The OPC is an Officer of Parliament, who reports directly to the House of Commons and the Senate. The Commissioner works independently from any other part of the government to investigate complaints from individuals with respect to the federal public sector and the private sector.

The OPC has developed an Information Management / Information Technology (IM/IT) Strategy for 2014-2017, as well as a separate more detailed 2015 IM/IT plan. Governance bodies in place in relation to IM/IT are the OPC Senior Management Committee (SMC), composed of Director General (DG) level representative, as well as the Change Control Board (CCB), composed of manager-level representatives. The Director of IM/IT acts as the Chief Information Officer (CIO) and reports to the Director General of Corporate Services at the OPC. This group includes 22 FTE's with an annual budget of approximately $1.7M in salaries and $1.1M in operating budget.

Despite being a relatively small organization, because of the nature of its work and strategic mandate the OPC has indicated its belief in having a robust IT infrastructure that promotes highly effective operations while ensuring a strong IT security posture.

The OPC has experienced significant growth over the last decade, and a number of significant events have impacted IM/IT in recent years. A move to a new facility occurred in February 2014, and in fiscal year 2014-15 the OPC performed an organization-level Threat and Risk Assessment (TRA) in order to evaluate the security threats and risks to OPC information, programs, systems, services and physical spaces.

The preliminary objective of the audit was to provide assurance to the Commissioner on the adequacy and effectiveness of governance, risk management and controls supporting the OPC's IM and IT processes. Based on the Planning Phase risk assessment, the scope of the audit was defined to include IM/IT governance processes, which included the governance over IM/IT HR capacity, IM/IT applications, change management for IT systems, and IM/IT-enabled project management processes.

Summary of Findings

The key findings with regards to the audit are provided below.

Strengths

- The OPC has developed an IM/IT Strategy for 2014-17 that establishes the OPC's IM/IT direction and aligns with OPC's corporate priorities and vision.

- The OPC IM/IT team is an experienced and skilled team that is delivering on a high volume of IM/IT initiatives.

- The OPC has developed project documentation, including Project Charters, project plans and functional requirements, for the large IM/IT-enabled projects reviewed as part of the audit. This included Ci2 Renewal, which is a case management system; and Officium, which is an electronic document and records management system.

- To increase the adoption of Officium within the OPC, as well as the user experience, IM/IT has recently undertaken extensive activities related to communication and change management with end users related to the implementation of the electronic documents and records management system.

Findings

- Although the OPC has developed an IM/IT Strategy (along with a supporting IM/IT Plan), these documents have not been formally discussed with, or approved by, senior management. In addition, there is no formalized process for regular communication/updates between IM/IT and senior management.
- Business application owners have not been formally identified or defined for any of the OPC's IT applications. In addition, the CCB is currently functioning as a management-level IM/IT committee rather than a change advisory board that defines how changes to IT applications are approved.
- There is no formalized IM/IT project management framework, including a formalized program for reporting benefits realization to senior management.

Conclusion

Based on the aforementioned observations and overall scope of the audit, the OPC has moderate issues related to the effectiveness of its current IM/IT governance processes. The recommendations included in this report are intended to further strengthen these processes. Management responses are included at the end of each finding.

This report and audit were conducted for OPC management purposes. Use of this report for other purposes may not be appropriate.

Statement of Conformance

In our professional judgment, sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the opinion provided and contained in this report. The opinion is based on a comparison of the conditions, as they existed at the time, against pre-established audit criteria that were agreed with management. The opinion is applicable only to the processes examined. The audit was conducted in accordance with the Internal Auditing Standards for the Government of Canada. The evidence has been gathered to provide senior management with reasonable assurance of the accuracy of the conclusions drawn from this audit.

2. Audit Objective, Scope and Approach

Background

The Office of the Privacy Commissioner of Canada (OPC) is responsible for overseeing compliance with both the *Privacy Act*, which covers the personal information-handling practices of federal government departments and agencies, and the *Personal Information Protection and Electronic Documents Act (PIPEDA)*, Canada's federal private-sector privacy law.

The OPC is an Officer of Parliament, who reports directly to the House of Commons and the Senate. The Commissioner works independently from any other part of the government to investigate complaints from individuals with respect to the federal public sector and the private sector.

The Commissioner is an advocate for the privacy rights of Canadians and his powers include:

- Investigating complaints, conducting audits and pursuing court action under two federal laws;
- Publicly reporting on the personal information-handling practices of public and private sector organizations;
- Supporting, undertaking and publishing research into privacy issues; and,
- Promoting public awareness and understanding of privacy issues.

The OPC has developed an IM/IT Strategy for 2014-2017, as well as a separate more detailed 2015 IM/IT plan. Governance bodies in place in relation to IM/IT are the OPC Senior Management Committee (SMC), composed of Director General (DG) level representative, as well as the Change Control Board, composed of manager-level representatives.

The Director of IM/IT acts as the Chief Information Officer (CIO) and reports to the Director General of Corporate Services at the OPC. This group includes 22 FTE's with an annual budget of approximately $1.7M in salaries and $1.1M in operating budget. IM/IT is responsible for providing IM/IT advice and direction, and for managing, coordinating, monitoring and reporting on all IM/IT investments throughout the IM/IT lifecycle.

Despite being a relatively small organization, because of the nature of its work and strategic mandate the OPC has indicated its belief in having a robust IT infrastructure that promotes highly effective operations while ensuring a strong IT security posture that is compliant with Treasury Board security policy requirements.

The OPC has experienced significant growth over the last decade, and a number of significant events have impacted IM/IT in recent years. A move to a new facility occurred in February 2014, and in fiscal year 2014-15 the OPC performed an organization-level Threat and Risk Assessment (TRA) in order to evaluate the security threats and risks to OPC information, programs, systems, services and physical spaces.

Audit Objective and Scope

The preliminary objective of the audit was to provide assurance to the Commissioner on the adequacy and effectiveness of governance, risk management and controls supporting the OPC's IM and IT processes.

The Planning Phase of the audit consisted of a broad IM/IT risk assessment for the OPC, which included conducting a risk workshop that included representatives from IM/IT and all of the Branches. Based on the risk assessment, the scope of the audit was defined to include IM/IT governance processes, which included the governance over IM/IT HR capacity, IM/IT applications, change management for IT systems, and IM/IT-enabled project management processes. The audit period for this audit was from April 1, 2013 to December 31, 2014.

Audit Approach

The approach and methodology to be used for the audit is consistent with the Internal Audit standards as outlined by the Institute of Internal Auditors (IIA), and is aligned with the Internal Audit Policy for the Government of Canada (GoC).

As an Agent of Parliament, the OPC works independently from the Government of Canada and although it is not obligated to follow the management improvement initiatives put forward in the Federal Public Service, it intends to maintain consistency with these practices. The OPC is firmly committed to achieving a standard of organizational excellence, applying sound business management practices, and continually improving its performance. Consequently, the following control frameworks were leveraged for the audit:

- Framework of Core Management Controls and Audit Criteria (CMC) established by the Office of the Comptroller General of Canada (OCG)
- Management Accountability Framework (MAF) that sets out the Treasury Board's expectations of senior public service managers for good public service management

Other criteria were also included to ensure appropriate coverage related to the scope of the audit.

The audit included an extensive Planning Phase, which initially considered the OPC's entire IM/IT Risk Universe. The preliminary risks were identified through interviews and document review, and these were developed into a set of risk statements that were discussed and voted on at a risk workshop, attended by representatives across the various Branch of the OPC. For the purposes of the workshop, the residual risk was considered, that is the level of risk as determined by workshop participants after the controls and practices that participants believed to be in place at the time of the workshop were considered. Based on risks identified in the Planning Phase of the audit, a risk-based audit program was developed to detail how the audit objective, criteria and risks would be addressed. The audit program included the following procedures:

- Interview with the Director IM/IT Services to further understanding on specific aspects of the IM/IT processes (refer to Appendix A);
- Interviews with Branch Directors to gather perspectives on IM/IT topics (refer to Appendix A);
- Review of the current and revised Terms of Reference for governance-related committees;
- Review of agendas and meeting minutes for governance-related committees;
- Review of IT project management processes, including documentation developed for the Officium and Ci2 projects; and,
- Review of IM/IT communication artefacts (e.g. newsletters, emails).

The audit was conducted within the following timelines:

- Planning Phase: October 2014 – November 2014
- Conduct Phase: November 2014 – December 2014
- Reporting Phase: January 2015 – February 2015
- Presentation to the OPC Audit Committee: March 2015

3. Findings and Recommendations

Strengths Noted

The following strengths were noted with regards to the current approach to applied research:

- The OPC has developed an IM/IT Strategy for 2014-17 that establishes the OPC's IM/IT direction and aligns with OPC's corporate priorities and vision.
- The OPC IM/IT team is an experienced and highly skilled team that is delivering on a high volume of IM/IT initiatives.
- The OPC developed project documentation, including Project Charters, project plans and functional requirements, for the large IM/IT-enabled projects reviewed as part of the audit (i.e., Ci2 Renewal, which is a case management system; and Officium, which is an electronic document and records management system).
- To increase the adoption of Officium within the OPC, as well as the user experience, IM/IT has recently undertaken extensive activities related to communication and change management with end users related to the implementation of the electronic documents and records management system.

Audit Findings

Finding #1: IM/IT Strategic Planning

IM/IT is critical to ensure corporate priorities are achieved, as such the audit team expected to find[1] *an overall IM/IT Strategy that was aligned to OPC's corporate priorities and vision, developed through ongoing consultation with business areas and approved by senior management. It was further expected that senior management would be regularly updated on IM/IT plans and initiatives. For an organization the size of OPC, IM/IT governance and management activities do not necessarily require numerous processes and levels of approval, but should occur in a formal and consistent* manner.

The OPC has developed a 2014-17 IM/IT Strategy (along with a supporting 2015 IM/IT Plan) that is consistent with the OPC's corporate priorities and vision. While IM/IT solicited input from each business area (through discussions between the IM/IT Director and Directors General of each Branch) to develop the strategy and plan, they have not been formally discussed with, or approved by, senior management (as of December 31, 2014). The IM/IT Director noted that comments on the draft strategy were only provided by one Branch.

A draft IM/IT Strategy workflow has been developed by IM/IT to describe the process for IM/IT Strategy development; however, the document has not been approved by senior management. A review of agenda items for the OPC Senior Management Committee (SMC) during the audit period indicated that

[1] For additional information refer to COBIT 5 processes related to Evaluate, Direct and Monitor (EDM), for instance EDM01 Ensure governance framework setting and maintenance, which includes the governance practice EDM01.02 Direct the governance system that states **"***Inform leaders and obtain their support, buy-in and commitment. Guide the structures, processes and practices for the governance of IT in line with agreed-on governance design principles, decision-making models and authority levels. Define the information required for informed decision making".*

discussion of IM/IT Strategy and planning was not included as a formal agenda item for any of the SMC meetings. It was noted that the 2014-17 IM/IT Strategy was scheduled for discussion at SMC in May 2014, but given other priorities, it was postponed as an agenda item.

The 2015 IM/IT Plan outlines the current and planned IM/IT projects, including estimated level of effort and timing for each project. Based on the estimated resource allocation, four IM/IT positions within the OPC are showing a planned utilization of over 100%, indicating that either the number or size of IMIT initiatives and/or the level of resources may need to be revisited. A separate Project List is used to track projects in progress; however, it does not capture the actual level of effort, nor is there an ongoing reconciliation between the estimated level of effort and the actual level of effort that has been expended on current and completed initiatives. Project status and potential resource constraints and risks have not been formally reported to the SMC.

Impact

Without an approved IM/IT Strategy and IM/IT Plan, or regular formal communication/updates between IM/IT and senior management, there is a risk that IM/IT priorities are not aligned with those of senior management. Furthermore, senior management may not understand IM/IT risks and constraints, for example the prioritization of IM/IT initiatives based on resource constraints, or implementation issues related to initiatives that require senior management intervention. Traditionally IM/IT at the OPC has been very responsive to any request from business areas, and IM/IT planning and resource allocation has been informal in nature. In the context of the current more resource-constrained environment at the OPC, and the heavy workload of IM/IT, it is important for senior management to understand IM/IT's capacity to meet the identified priorities of the OPC. The lack of formal or effective communication has also lead to questions related to decisions that were made several years ago, for example the selection of SharePoint as the basis for OPC's document management system. Given that some within senior management feel they were not fully involved or understood the decision making process, questions related to this decision continue to be asked. This has potentially resulted in increased user resistance and hampered user change management activities.

Recommendation

1. It is recommended that the DG Corporate Services Branch ensure that IM/IT Strategy and Plans are discussed and formally approved by senior management in a timely fashion, and that an update on the status of the approved IM/IT Strategy and Plans are also regularly discussed with senior management. The purpose of status updates should be to confirm that current and planned IM/IT-related initiatives remain in line with the OPC's overall priorities and vision, and to discuss current resource allocation decisions to ensure prioritization is done to optimize value for the OPC.

Management Response and Action Plan	Responsibility / Deadlines
We agree with the recommendation and will undertake the following: 1. Present the IM/IT Strategy Workflow to SMC to ensure that: a. there is a common understanding of the process for developing the strategy and more specifically, the role of SMC within this process. b. confirm the approach for keeping SMC informed of updates or deviations from the IM/IT Strategy and Plans going forward.	DG, Corporate Services Branch (April/May 2015)

Management Response and Action Plan	Responsibility / Deadlines
2. Present the 2015-16 IM/IT Strategy and Plans to SMC for approval. 3. Provide quarterly IM/IT updates to SMC.	

Finding #2: Application Oversight and Change Control

The audit team expected to find[2] that key applications were formally 'owned' by designated business owners. Although IM/IT is responsible for ensuring the appropriate maintenance and operations of applications, it is ultimately the business that is accountable for defining the expected business outcomes (i.e., requirements) for the application and for approving decisions related to how the applications support the business. Furthermore, the audit team expected that a formalized process was implemented to identify, capture, analyze, prioritize and approve application change requests. This process should be enabled by IM/IT but with accountability ultimately with the identified IT application business owners.

Business owners have not been formally identified, or their role defined, for any of the OPC's IT applications. Business areas have looked to IM/IT to take on the development and support of IT applications, as well as management activities related to them, including change requests.

A formal change management process framework for IT application change requests was documented in August 2014. Senior management has yet to approve the framework. The framework outlined that IM/IT would prioritize user submitted change requests in order to be submitted to the Change Control Board (CCB) for final approval. Approval of change requests by the CCB has yet to occur. The documented change management process was leveraged from a similar process that had been previously utilized for the Ci2 Renewal project. Since the completion of the Ci2 Renewal project in 2013, change requests were generally handled in an informal fashion.

As of December 31, 2014, the CCB had met four times since the formal change management process was documented. The Terms of Reference of the CCB indicates its role is to oversee the implementation and management of changes associated with business IT applications within the OPC. The Terms of Reference do not outline, and the CCB has not further defined, how change requests will actually be approved, including whom should be voting members (and how this may depend on the application to which the change request applies), and what constitutes quorum and the actual approval of a change request. The CCB includes over 28 management-level individuals from throughout the OPC, with all members listed in the Terms of Reference as both contributor / approver. Discussions at the CCB to date have been related to providing information on IM/IT initiatives as opposed to specific change requests, and no decisions of the CCB has been recorded in the minutes.

Impact

Without formally defining IT application business owners, management decisions related to applications are left to IM/IT resources, who may not have sufficient knowledge of the business processes supported by the IT applications. Business areas must understand the strong link between business processes and the IT applications that support them, to ensure the impact on IT applications are considered when business processes are changed. For instance, changing how data may be captured or coded in existing IT applications.

The CCB is currently functioning as a management-level IM/IT committee that vets information prior to its presentation to the SMC. Although this is a useful function, it does not fulfill the requirements needed for a change advisory board, which should define how changes to IT applications are approved. This includes identifying those stakeholders that need to approve changes, for example the IT application business owner and supporting functional roles such as security and privacy. Without a well-defined change advisory processes, the change process may be both inefficient (given the number of individuals

[2] For additional information refer to COBIT 5 processes related to Build, Acquire and Implement (BAI), for instance BAI06 Manage Changes, which includes the governance practice BAI06.01 Evaluate, prioritise and authorise change requests, which indicates "*Evaluate all requests for change to determine the impact on business processes and IT services, and to assess whether change will adversely affect the operational environment and introduce unacceptable risk. Ensure that changes are logged, prioritised, categorised, assessed, authorised, planned and scheduled*". Although IMIT staff are responsible for these processes, it is clearly senior management and their delegated process owners that are accountable for these processes.

currently attending CCB) as well as may not fully consider all the risks (given unclear roles and responsibilities).

Recommendations

2. It is recommended that the DG Corporate Services Branch ensure that business owners are formally assigned for each key IT application (i.e., Ci2, Officium, finance and HR systems), with their roles and responsibilities formally defined, communicated, and accepted by the business owner.

Management Response and Action Plan	Responsibility / Deadlines
We agree with the recommendation. IM/IT will develop a model that assigns Branch ownership of the business aspect of the applications but not the funding of the updates or upgrades of the applications. IM/IT will work with the Branch to seek funding where required. Specifically, we will undertake the following: 1. Develop an approach to formally define, assign and communicate the roles and responsibilities for the OPC's key applications. The approach taken will focus on effectively supporting the IM/IT operations while also considering the operational realities and limitations of a small organization. 2. Discuss and formally obtain approval by those assigned responsibilities for key systems.	DG, CSB (September 2015)

3. It is recommended that the Director IMIT ensure the IT application change review and approval function of the CCB is further defined, including providing guidance on which members are voting members and their role in the approval of changes for each key IT application.

Management Response and Action Plan	Responsibility / Deadlines
We agree with the recommendation and will undertake the following: 1. Review the current OPC Governance Model for IM/IT, including the composition, roles and responsibilities of the Change Control Board and its reporting relationship to SMC. 2. Revise the Terms of Reference of the Change Control Board to clearly define roles and decision-making responsibilities. 3. Present the revised ToR to the SMC and to the Change Control Board for approval to ensure roles and responsibilities are understood and formally accepted	Director, IM/IT (September 2015)

Finding #3: IM/IT-Enabled Project Management

The audit team expected to find[3] *a formal project management framework that included an approach for the completion of IM/IT-enabled projects, including formal controls for the review and approval of projects by senior management at key phases (i.e., planning, execution, and deployment). Furthermore, it was expected that the framework considers how the expected benefits of a project are identified and revisited at project completion to determine if they were realized. It was also expected that a comprehensive people change management plan would be developed and executed for any large scale project impacting the majority of staff within the OPC. For an organization the size of OPC, IMIT-enabled project management activities do not require numerous processes and levels of approval, but should ensure key areas within project management methodology are considered, including formal approval by senior management at key project milestones.*

The OPC does not have a formal project management framework. Despite this, the OPC developed project documentation, including Project Charters, project plans and functional requirements, for the large IM/IT-enabled projects reviewed as part of the audit (i.e., Ci2 Renewal and Officium). Although project artifacts were developed, evidence of senior management approval at key milestones of the projects does not exist.

Although success criteria were included in the Project Charter for Officium, these criteria were high level and do not lend themselves to measurement, for example "*The new environment is stable"* and "*All OPC users were properly trained on the new technology*." Although Officium has been implemented for over a year, the degree to which the success criteria have been met, has not been measured or reported to senior management.

The Officium project invested in extensive training and has comprehensive training material on the OPC Intranet. This, however, was not supported by a detailed people change management and communications plan. Such a plan would have included a stakeholder analysis that would have determined stakeholder information needs and how groups should be engaged throughout the evolution of the project, including an integrated schedule that identified for each stakeholder group the appropriate content, media, and timing of training and communication material. OPC's HR Branch has an extensive framework and templates for change management; however, they were not engaged at the outset of the project. A working group of users from across the OPC was implemented during the project, but was disbanded after Officium was implemented.

IM/IT has recently undertaken communication and change management activities with Officium end users, including conducting a survey of users and engaging with the OPC Communications Branch to create communication material. A more formal program of measuring the adoption of Officium (number of users and records in each Branch) has not been undertaken, including reporting these metrics to senior management, with action plans to address those areas of concern.

Impact

Without a formal project management framework and appropriate senior management oversight, including the consideration of the benefits realized, there is a risk that projects will not be able to be delivered against their objectives, timelines and budgets. The lack of a formal, comprehensive change

[3] For additional information refer to COBIT 5 processes related to Build, Acquire and Implement (BAI), for instance BAI01 Manage Programmes and Projects, which includes the governance practice BAI01.01 Maintain a standard approach for programme and project management, which indicates "Maintain a standard approach for programme and project management that enables governance and management review and decision making and delivery management activities focussed on achieving value and goals (requirements, risk, costs, schedule, quality) for the business in a consistent manner." Also refer to process BAI05 Manage Organisational Change Enablement, which includes the governance practices BAI05.01 Establish the desire to change, which indicates "Understand the scope and impact of the envisioned change and stakeholder readiness/willingness to change. Identify actions to motivate stakeholders to accept and want to make the change work successfully."

management program, including engagement with the business and the ability of users to continue using the old system, may have contributed to a slower adaptation of Officium. The recent Officium user survey indicated that 49% of users are using the system 'always or often' and that two-thirds of users want more training. It should be noted that given the integration between Officium and Ci2, that users may be accessing Officium functionality; for example, cases saved through the Ci2 case management system are saved in Officium, without knowing that they are actually utilizing Officium.

Recommendations

4. It is recommended that the Director IM/IT develop a high-level project management framework which includes gates where the approval of OPC senior management is required, and how benefits realization and change management activities will be included in integrated project planning. This includes post implementation monitoring by the business to determine if identified project benefits were achieved.

Management Response and Action Plan	Responsibility / Deadlines
We agree with the recommendation and will undertake the following: 1. Develop a high-level project management framework that will be applied to large-scale IM/IT projects. The framework will reflect the small size of the OPC, and will outline when SMC approval will be sough and how benefits realization and change management activities will be included in the integrated project planning. In developing the framework, IM/IT will leverage existing tools such as the OPC change management strategy and project planning tools, and will consult with the Change Control Board. 2. Present the framework to SMC for approval.	Director, IM/IT (March 2016)

5. It is recommended that the Director IM/IT continue to work further with the Branches to ensure there is a comprehensive people change management plan, including the support and monitoring that is required, to sustain the implementation of Officium.

Management Response and Action Plan	Responsibility / Deadlines
We partially agree with the recommendation. At this time, since the Officium is now in full production and all active documents have been migrated, the need for a formal change management plan is no longer required. However, we recognize the need for specific additional actions to ensure full buy-in of the new system. IM/IT will support and continue with training and implementation of the action plan while reviewing options to improve usage and understanding of the new application. 1. Evaluate success of migration to Officium through	Director, IM/IT with branches (June 2015)

usage of new system by employees. 2. Develop additional mechanisms to further promote and facilitate use of Officium for employees who have not fully committed to new business tool.	

Appendix A – Interviewees

Individuals who were interviewed as part of the internal audit process:

- Privacy Commissioner of Canada
- Director General/CFO, Corporate Services Branch
- Director General, Privacy Act Investigations
- Director General, PIPEDA
- Director General, Audit and Review
- Director General, Communications
- Senior General Counsel and Director General
- Director, Technology Analysis Branch
- Director, Policy and Research
- Director, Legal Services and Senior Counsel
- Director, ATIP and Chief Privacy Officer
- Director, IM/IT Services
- Director, Financial and Administrative Services
- Director, Human Resources Management
- Manager, Information Management Programs and Services
- Manager, Privacy Investigations Branch
- Manager, Business Analysis, Systems Management and Support
- Manager, Financial Planning, Budgeting, Reporting and Costing
- Manager, Accounting Operations, Policy and Systems
- Malware Analyst, Corporate Services Branch
- Senior Privacy Investigator, Toronto Office
- Technical Analyst, Information Management Programs and Services
- Complaints Registrar, Privacy Investigations Branch

Appendix B – Audit Criteria

The following audit criteria were used for this audit:

Audit Criteria	CMC Reference
1. Governance and Oversight	
1.1 Effective oversight bodies have been established for IM/IT.	G-1, G-2
1.2 Roles and responsibilities for IMIT governance, planning, and initiatives have been clearly defined and communicated.	AC-1
1.3 Processes have been implemented for identifying, prioritizing, and approving changes related to the operations and maintenance of IT applications.	G-4, PR-1
2. IM/IT Direction and Planning	
2.1 IM/IT planning and investment decisions are based on input from senior management across the OPC and aligned with strategic and business planning.	G-4, PR-1
2.2 Contingency plans have been developed to ensure any IM/IT capability and capacity issues could be resolved in a timely and effective manner.	PPL-1, PPL-2
3. IM/IT Project Management	
3.1 Project management processes and controls are implemented to ensure projects can deliver against their objectives, timelines and budgets. This includes project benefits being clearly documented and an effective approach is in place to track against the realization of these benefits.	CFS-4