Employment and Social Development Canada
Emploi et Développement social Canada

Now and Tomorrow, Excellence in Everything We Do

Unclassified

Internal Audit Services Branch

Audit of the Departmental Control Framework for the Management of Personal Information (Privacy)

August 2015

SP-1107-01-16E

Canada

You can download this publication by going online: publicentre.esdc.gc.ca

This document is available on demand in multiple formats (large print, Braille, audio cassette, audio CD, e-text diskette, e-text CD, or DAISY), by contacting 1 800 O-Canada (1-800-622-6232). If you use a teletypewriter (TTY), call 1-800-926-9105.

PDF

Cat. No.: Em20-36/2016E-PDF
ISBN: 978-0-660-04158-2

ESDC

Cat. No. : SP-1107-01-16E

Table of Contents

Executive Summary 1
1.0 Background 3
1.1 Context 3
1.2 Audit Objective 3
1.3 Scope 3
1.4 Methodology 4
2.0 Audit Findings 4
2.1 Governance and Accountability 5
2.2 Stewardship of Personal Information 6
2.3 Culture, Training, and Awareness 8
2.4 Risk Management 9
2.5 Assurance of Compliance 10
3.0 Conclusion 11
4.0 Statement of Assurance 11
Appendix A: Audit Criteria Assessment 12
Appendix B: Glossary 13

Executive Summary

Employment and Social Development Canada (ESDC) programs require the collection, use and disclosure of detailed, and at times, sensitive personal information. With the breadth of ESDC's mandate, the Department has one of the largest personal information holdings in the Government of Canada. Although the importance of safeguarding the personal information of Canadians is a departmental priority, ESDC was exposed in 2012 when an external hard drive and a USB[1] storage device containing personal information were lost.

Following the breach, the Office of the Privacy Commissioner conducted an investigation and issued recommendations that were addressed by ESDC. The Department had already been in the process of reviewing its Privacy Management Framework (PMF) which included a multi-year privacy renewal initiative. The Privacy Renewal Action Plan included the development of a revised Departmental Policy on Privacy Management (DPPM) which was implemented on April 1, 2014. The DPPM and its directives set out the application of the *Privacy Act,* R.S.C. 1985, c. P-21, the Privacy Regulations, the *Department of Employment and Social Development Act (DESD Act)* "Privacy Code[2]", the Treasury Board Privacy Policy and Directives, and the ESDC Code of Conduct, with the aim of fostering a robust policy regime for the protection and judicious use of personal information.

ESDC's 2014–2015 Corporate Risk Profile (CRP) identifies Privacy/Security of Information as one of the top five departmental risks. The main risk drivers include: the high volume of personal and sensitive information[3], the high number of Information Sharing Agreements (ISAs) as well as the current privacy and information management (IM) methods and practices.

Audit Objective

The objective of this audit was to assess the adequacy and effectiveness of the ESDC PMF to safeguard the personal information of Canadians.

Summary of Key Findings

- ESDC has a well-defined and functioning governance structure in place to support the Department's Privacy Framework in the management and protection of personal information. This governance structure includes defined accountabilities and a dedicated committee to govern privacy management. The Privacy and Information Security Committee (PISC), the main governance body, is seen by managers interviewed to be too transactional in nature. There is an opportunity for PISC to be more horizontally focused on privacy and security issues and risks.
- The management of ISAs remains a risk as not all agreements containing information sharing provisions have been identified, assessed and managed.
- Risk processes for Privacy Impact Assessments (PIA) could be strengthened to provide a comprehensive and timely view of Information Technology (IT) risks identified in PIAs.

---

1 USB is an acronym that stands for Universal Serial Bus which is a type of computer port that can be used to connect equipment to a computer.

2 Part 4 of the enabling legislation, often referred to as the Department's Privacy Code, applies more stringent rules on the Department which supersedes the *Privacy Act,* R.S.C. 1985, c. P-21, with respect to the sharing of information.

3 Sensitive information is personal information that requires an extra level of protection and a higher duty of care.

- Relevant documentation from the privacy policy suite is difficult to locate on the document repositories on iService[4] and the intranet.
- Although the Departmental Security Officer (DSO) and the Chief Privacy Officer (CPO) manage privacy incidents on a transactional basis, there is no systematic reporting that would support effective trend analysis at the departmental level. Reporting on privacy incidents and trend analysis would allow the DSO, CPO, senior management and PISC to make informed strategic and horizontal decisions on the direction of the privacy program and validate the successes or shortcomings of the initiatives that have been implemented.
- Mandatory privacy training and communication efforts on privacy management to the Department's employees have been satisfactory. The Stewardship of Information and Workplace Behaviours (SIWB) training is seen as a departmental best practice for integrating privacy principles with IT and IM principles.
- ESDC is monitoring the Framework for the management of personal information. This includes a dedicated governance body and an internal audit regime. There is also monitoring through exercises such as the Program-led Privacy Action Plans (PLPAPs).
- Monitoring of access controls continues to be a challenge until the actions to address the gaps identified in past audits have been fully implemented.

Audit Conclusion

The audit concluded that ESDC's PMF is adequate to address most privacy-related concerns. There are processes and controls in place that are sustainable over time, including a dedicated governance body and a policy suite for privacy management. However, there are still areas of the PMF that could be improved. Opportunities exist to further integrate the PIA, Security Assessment and Authorization (SA&A) and Threat and Risk Assessment (TRA) processes, to institute consolidated privacy incident trend reporting, and to improve the stewardship of ISAs.

Recommendations

1. The Department should ensure that the current ISA inventory is completed in a timely manner and that all agreements containing information sharing provisions are identified, assessed and managed on an ongoing basis.

2. The DSO in partnership with the Corporate Secretary, in her capacity as CPO, should ensure that a mechanism is put in place to consolidate privacy incident reporting and trends across the Department.

3. Innovation, Information, and Technology Branch (IITB), in partnership with the Corporate Secretary, in her capacity as CPO, should ensure that approaches to the PIA, SA&A and TRA processes are better aligned and integrated to provide a comprehensive view of privacy and security risks (physical and IT) in a consistent and timely manner.

[4] iService is part of ESDC's intranet and is comprised of on-line information from enabling branches to allow employees to search for up-to-date information.

1.0 Background

1.1 Context

ESDC programs require the collection, use and disclosure of detailed, and at times, sensitive personal information. With the breadth of ESDC's mandate, the Department has one of the largest personal information holdings in the Government of Canada. The importance of safeguarding the personal information of Canadians is a departmental priority and significant resources and management attention are spent on this issue.

The Department has been in the process of reviewing its PMF which included a multi-year privacy renewal initiative. As a result of the Privacy Renewal Action Plan a revised DPPM was implemented on April 1, 2014. The DPPM and its directives set out the application of the *Privacy Act,* R.S.C. 1985, c. P-21, the Privacy Regulations, the *DESD Act* "Privacy Code[5]", the Treasury Board Privacy Policy and Directives, and the ESDC Code of Conduct, with the aim of fostering a robust policy regime for the protection and judicious use of personal information.

The DPPM applies to all employees, agents and contractors of ESDC where the Deputy Minister (DM) of Employment and Social Development is the designated Accounting Officer. Included in the Policy are defined roles and responsibilities for all employees, including the functional responsibilities of the Corporate Secretariat, a role that includes being CPO of the Department.

ESDC's 2014–2015 CRP identifies Privacy/Security of Information as one of the top five departmental risks. The main risk drivers include: the high volume of personal and sensitive information[6], the high number of ISAs as well as the current privacy and IM methods and practices.

1.2 Audit Objective

The objective of this audit was to assess the adequacy and effectiveness of the ESDC PMF to safeguard the personal information of Canadians.

1.3 Scope

The scope of this audit included departmental policies, processes, and practices related to ESDC's PMF between April 2013 and December 2014. Specifically, the audit examined the Framework in terms of the following pillars: Governance and Accountability; Stewardship of Personal Information; Culture, Training, and Awareness; Risk Management; and Assurance of Compliance. These pillars are consistent with the ten Generally Accepted Privacy Principles[7].

---

5 Part 4 of the enabling legislation, often referred to as the Department's Privacy Code, applies more stringent rules on the Department which supersedes the *Privacy Act,* R.S.C. 1985, c. P-21, with respect to the sharing of information.

6 Sensitive information is personal information that requires an extra level of protection and a higher duty of care.

7 Developed by the American Institute of Chartered Professional Accountants and the Canadian Institute of Chartered Accountants in 2009, the principles and criteria in the document were developed based on international privacy regulatory requirements and best practices. The ten principles are: Accountability; Identifying Purposes; Consent; Limiting Collection; Limiting Use, Disclosure and Retention; Accuracy; Safeguards; Openness; Individual Access; and Challenging Compliance.

1.4 Methodology

The audit was conducted using a number of methodologies, mainly interviews with key members of the ESDC privacy regime including senior management, regional and program executives, documentation review, and analysis.

The Corporate Secretary, whose position includes the role of CPO, was the main stakeholder in this engagement. The Integrity Services Branch, IITB, Legal Services, and selected programs and regions were also consulted to offer a comprehensive view of the departmental PMF.

While the focus of this audit was to assess the PMF, it is important to note that there are also various audit projects from the approved 2014–2017 Risk-Based Audit Plan that will further assess how specific components of the Framework are being applied. These engagements were considered by the audit team in finalizing the audit scope.

The audit work was conducted between October 2014 and January 2015.

2.0 Audit Findings

To achieve ESDC's personal information protection objectives, and to build privacy into the design and architecture of programs, services, systems and technologies, the Department has established an Integrated Framework for Privacy Management consisting of the following pillars:

- **Governance and Accountability:** Established roles, responsibilities, and mechanisms to support the Department's conformance to legal requirements, regulations, policies, standards, and public expectations.

- **Stewardship of Personal Information:** Appropriate privacy protection to safeguard personal information through its life-cycle.

- **Culture, Training, and Awareness:** A privacy-respectful culture where employees, partners, and delivery agents understand their privacy obligations and are aware of tools, resources, policies, and processes related to privacy and personal information protection.

- **Risk Management:** Deliberate and systematic efforts to limit the probability and impact of negative events and maximize opportunities through risk identification, assessment, and prioritization.

- **Assurance of Compliance:** Formal processes and practices to ensure adherence to privacy legislation, policies and standards.

The following presents strengths and opportunities for improvement as they relate to the Department's Framework for the management of personal information.

2.1 Governance and Accountability

Governance bodies are in place and accountabilities are defined to support the management and protection of personal information

The DPPM, implemented in 2014, states that the DM of Employment and Social Development is responsible for the Department's compliance with all statutes and Treasury Board policies and directives concerning the management and protection of personal information. This accountability is reaffirmed in the Department's *Delegation Order*, signed in August 2010 which is currently being updated.

The DPPM defines the roles and responsibilities for privacy, further stating that all employees are responsible for ensuring the safeguarding and protection of personal information under their custody and control. The DPPM also specifies functional responsibilities and accountabilities for senior management directly involved in administering the Framework. These include the CPO, the DSO, and the Departmental IT Security Coordinator.

The CPO is designated as the Department's functional authority and senior advisor on privacy matters, and is accountable for the continual development and oversight of the DPPM, its associated directives and instruments, and the privacy management program. Having the DPPM describe the functional roles of the CPO, DSO and Departmental IT Security Coordinator represents an important effort in the integration of the functional areas in the management of personal information.

The DPPM also defines the oversight committees that support the protection of personal information and the consequences for violation of the DPPM or related statutes, policies and procedures. PISC, a sub-committee to the Corporate Management Committee (CMC), serves as the main governance body for setting the mandates for privacy and the protection of personal information, including policy development and supporting the horizontal coordination and prioritization of issues, plans and strategies. The committee is co-chaired by the CPO and the DSO and is comprised of Directors General from ESDC branches. In addition, there is regional representation on the committee through Executive Directors.

PISC's membership provides a strategic and horizontal privacy view to issues and risks and demonstrates the Department's commitment to integrate privacy, IT security and IM. Key PISC activities in 2014 included: providing guidance on five new IM/IT directives in response to the ESDC IM/IT Security Plan, reviewing the new SA&A process, implementing a new PIA prioritization methodology, reviewing and approving an Annual Report to Parliament on the Administration of the *Privacy Act* and reviewing relevant external audit reports that touch on privacy.

CMC receives regular updates from PISC on the progress of privacy, IT security, IM and physical security and approves privacy-related documentation. Specific items discussed at CMC dating back to December 2013 include: review and approval of annual PISC priorities, Directive on Public Interest Disclosure, update on the Departmental IT Security Program, Corporate Secretariat Plan, and Integrated Departmental Security Framework. Overall it was found that privacy-related matters are being reported effectively to CMC.

Two of the main mechanisms that the Department utilizes as part of its Privacy Framework are PIAs and ISAs. PIAs are a requirement of the Treasury Board Secretariat for any programs or initiatives that require the use of or transmission of personal information. ESDC's approach in developing the PIAs is seen as a best practice, within the Department, to ensure that each program or initiative has a thorough analysis of the privacy risks and associated mitigation strategies in place before a program or initiative can use personal information. An ISA is a written record of understanding between ESDC and third parties, such as other government departments or provincial and municipal governments, that outlines the terms and conditions under which personal information is shared between the parties.

As part of the PISC's mandate, the committee reviews, offers feedback and recommends approval of all PIAs and ISAs. The audit team observed that PIAs and ISAs were regular agenda items requiring a great deal of attention at PISC meetings. Therefore, PISC is sometimes seen by committee members interviewed as being too transactional, paying more attention to the review and approval of PIAs and ISAs rather than addressing broader horizontal issues associated with PIAs and ISAs.

Through interviews with regional and program executives who sat on PISC, it was found that the emphasis on review and approval of PIAs and ISAs caused members to be less engaged and overburdened with documentation. Committee members often receive PIA and ISA documentation only one to two business days prior to committee meetings, making it challenging for PIAs and ISAs to be fully reviewed and for members to provide meaningful feedback. An opportunity exists for PISC to review the current approach and focus of the committee in order to address horizontal privacy and security issues and risks.

2.2 Stewardship of Personal Information

Accessibility of relevant privacy documents needs improvement

The DPPM provides an overview of ESDC's PMF, which discusses the ten privacy principles that provide the basis upon which privacy policies, directives and procedures are founded. The DPPM aligns with the *DESD Act* (including the Privacy Code within the *DESD Act*) and the *Privacy Act,* R.S.C. 1985, c. P-21. ESDC has also implemented a number of directives to support the policy suite and the overall stewardship and protection of personal information.

The Privacy Management Division and CPO have created a 'Stewardship of Information' iService[8] page on the departmental intranet to provide all employees with access to the Department's Framework for the management of personal information, including copies of relevant policies, directives and other guidance. Links to mandatory training, and contact information for privacy questions and issues are provided.

Despite the Department's best effort to communicate its privacy policy suite, finding privacy-related documents is difficult on iService and the intranet. The audit observed that searching for relevant privacy-related documentation was challenging. For instance, the DPPM was difficult to find using the search engines. Some additional important documents and links were found to be outdated.

It would be advisable for the Department to review the IM process including naming conventions, use of metadata[9], storage of documents and timely uploading to the intranet and other repositories, so that policies and guidance tools related to Privacy, Security, IT and IM can be easily found and accessed by ESDC employees.

Stewardship of ISAs remains a risk

ESDC collects, uses and discloses significant volumes of personal information to support the delivery of social and labour market programs and services. It also shares the personal information of its clients[10] where it has the legal authority to do so. The Department currently manages more than 500 known agreements (which contain information sharing provisions) between itself and other federal institutions, levels of governments and foreign institutions, as well as internal ESDC branches and regions. These agreements are called ISAs and they must meet the requirements of the *DESD Act*, Part 4 *(*referred to as the Privacy Code) and the *Privacy Act,* R.S.C. 1985, c. P-21. Part 4 requires the Minister's (or delegate)

8 iService is part of ESDC's intranet and is comprised of on-line information from enabling branches to allow employees to search for up-to-date information.

9 Metadata is data that defines and describes other data and it is used to aid the identification, description, location or use of information systems, resources and elements as per Treasury Board.

10 Client refers to internal and external service recipients.

approval of a written agreement with an organization outside the Department where protected personal information is shared. Per the delegation of authority instrument in place since 2010, the DM of ESDC has been delegated by the Minister the authority to sign agreements that contain information sharing provisions. There is also a process in place requiring all ISAs to be reviewed by PISC and recommended to the DM for signature. The risks associated with data sharing and ISAs rest with the current incomplete inventory of ISAs entered into by the Department.

In the 2014–2015 CRP, one of the main risk drivers for the 'Privacy/Security of Information' is the high number of ISAs involving personal information. The CRP stated that there was a risk that ESDC's personal and sensitive information may be inadvertently or inappropriately accessed, collected, used, disclosed, retained and disposed of by employees and third parties.[11]

To mitigate this risk CMC approved an ISA action plan in February 2014 to address privacy risks and control gaps. The plan included a strategy to compile an inventory of all ISAs, to assess them for compliance with the Privacy Code and to identify, triage and prioritize ISAs (using a risk-based approach) that require updating.

It was observed during related audit planning work and this audit engagement that a comprehensive repository of existing agreements is still outstanding. The Privacy Management Division is currently working with branches and regions to build an inventory of ISAs and to conduct a risk triage, in an effort to help branches and regions understand their priorities in complying with current legislative requirements. The continued effort to inventory ISAs is important to provide the Department with a sense of the magnitude of the number of ISAs in place.

Recommendation 1

The Department should ensure that the current ISA inventory is completed in a timely manner and that all agreements containing information sharing provisions are identified, assessed and managed on an ongoing basis.

Management Response

The Corporate Secretary, in her capacity as CPO and the Senior Assistant Deputy Minister of Strategic and Service Policy Branch concur with this recommendation. The Privacy Management Division will continue to manage ISAs until the program supporting the Chief Data Officer is developed in the fall of 2015.

Departmental privacy incident monitoring and reporting to PISC need improvement

There are various departmental branches involved in monitoring and reporting on privacy issues. The Privacy Management Division, within the Corporate Secretariat, prepares ESDC's Annual Report on the Administration of the *Privacy Act*, to highlight privacy management accomplishments and areas of concern/improvement. The report, tabled in Parliament, provides statistics on completed PIAs, requests for information under the *Privacy Act,* R.S.C. 1985, c. P-21, privacy training and awareness activities, public interest disclosures, complaints and investigations, and material privacy breaches.

IITB, in charge of managing IT Security, monitors on an ongoing basis the use of non-sanctioned external portable devices (e.g. USB storage devices, external hard drives). When an incident occurs with a non-sanctioned portable device, an email is sent from IT Security to the employee's manager explaining the

[11] 2014–15 Corporate Risk Profile, dated June 2014, page 11.

nature of the incident. Emails being sent from IT Security are for isolated incidents and are not systematically reported to governance bodies.

The DSO works in partnership with the CPO to maintain the Directive on How to Respond to Security Incidents Involving Personal Information and the Security Incident Reporting Protocol for the Department. The DSO Security Incident Management Unit (SIMU) has developed reference guides and tools to assist employees with security incident reporting. SIMU conducts internal tracking of all security incidents involving personal information by recording incident details and mitigations.

Although the DSO and the CPO manage privacy incidents on a transactional basis there is a lack of horizontal analysis and reporting which would be of benefit to the Department. Such systematic reporting and trend analysis would allow the DSO, CPO, senior management and PISC to make informed strategic and horizontal decisions on the direction of the privacy program and validate the successes or shortcomings of the initiatives that have been implemented.

Recommendation 2

The DSO, in partnership with the Corporate Secretary, in her capacity as CPO, should ensure that a mechanism is put in place to consolidate privacy incident reporting and trends across the Department.

Management Response

The Assistant Deputy Minister (ADM) of Integrity Services Branch and the Corporate Secretary, in her capacity as CPO concur with the recommendation. Technology is being developed to support privacy incident and trend reporting. Once completed by September 2015, quarterly reporting to the DSO, CPO and PISC will take place.

2.3 Culture, Training, and Awareness

Training and awareness programs have been established

Service Canada College developed the mandatory SIWB training that provides ESDC employees with a high-level, integrated overview of the departmental privacy program, including IT Security and IM. The objective of the SIWB training is to ensure that ESDC employees can demonstrate a basic understanding of their roles and responsibilities for the use and care of departmental and/or personal information and correctly apply the acquired knowledge. The training curriculum includes values and ethics, privacy roles, responsibilities, relevant policies, risks and threats, departmental security, IT security, IM, access to information and privacy requests. It also covers the consequences for not adhering to the prescribed privacy practices.

After taking the on-line ‘Stewardship’ course, employees are required to pass a test, complete a learning report, and complete a post-course evaluation. As of August 2014, training was taken by 98.7% of employees, virtually all of whom (99.9%) passed the test. The SIWB training manual provides reference material, all of which can be found on the departmental intranet/iService.

It is the audit team’s opinion that SIWB training is a departmental best practice as it integrates privacy principles with IT and IM principles.

Senior management continues to use multiple approaches to communicate the importance of managing and safeguarding personal information. Examples of initiatives include joint awareness sessions with the CPO, DSO and Director General of Strategy, Planning, Architecture and Management in IITB; Stewardship of Information intranet site; videos; emails from corporate communications; and awareness weeks.

However, the audit noted that there is a need for ongoing reinforcement of privacy principles. Regions and programs stated that privacy training was too high-level and less applicable to employees outside of National Headquarters (NHQ). Training that is more tailored to frontline staff would be more relevant to reinforce the privacy principles. Regions and programs stated that case studies and real life examples would be beneficial if included in the training.

Interviews during the audit revealed that there is 'communication fatigue' within the Department due to the frequency of communication and content that does not match the intended audience, particularly in regional operations. Lastly, concerns were raised whether communications are actually being absorbed by employees, questioning whether the communication mediums and reinforcement need to be re-evaluated.

It would be beneficial for management to continue to assess the effectiveness of the communication and training strategies to ensure the Framework for the management of personal information is being understood and applied across the Department. Approaches could include providing periodic case studies and reinforcement by managers through team discussions of privacy principles and applicability to their employees.

2.4 Risk Management

Departmental risk management includes privacy principles, however, risk processes for PIAs could be strengthened

ESDC has mechanisms in place to monitor privacy risk, including the Department's CRP. Currently Privacy/Security is one of the Department's top risks listed in the CRP and in branch/program risk registers. One of the main risk drivers of the Privacy/Security risk is the high number of ISAs in the Department. To help compile the CRP, each branch compiles risks to their programs into a risk register which is then funneled into the CRP. As part of this process senior management is interviewed, including the Corporate Secretary, to gather their thoughts on corporate-level risks.

The Department has, in addition to the CRP, other processes that assess risks related to the management and safeguarding of personal information at the program level, including PIAs, IT Security and Physical Security TRAs.

As per Treasury Board Secretariat's guidance, the key goal of a PIA is to effectively identify, communicate and mitigate privacy risks not addressed through other departmental mechanisms.[12] It is a cooperative process that brings together a variety of skill sets that include amongst others privacy, IT and physical security risks. A PIA is intended to contribute to senior management's ability to make fully informed policy, system design and contracting decisions.

Over the course of the audit, the team reviewed six of the 12 PIAs dating back to December 2013 which were presented to PISC in 2014. The audit team observed inconsistencies in the presentation of risk information ranging from: PIAs which included a thorough risk ranking of privacy and security risks; to PIAs which were supported by IT Security TRAs; and finally, to PIAs which included minimal ranking of risks and incomplete IT Security TRAs.

In an effort to improve the mitigation and monitoring of IT risks, ESDC proposed a new SA&A process in 2014 to replace the current TRAs for IT Security. The new SA&A process is expected to ensure that IT security risks are examined and mitigated before IT solutions are implemented. It is also expected to monitor risks throughout the life-cycle of that solution. Furthermore, the Department monitors risks through the implementation of PLPAPs. In 2011 the Department conducted a series of program risk assessments and developed PLPAPs in 2012–2013 to mitigate potential privacy risks that were identified. Risk assessments are currently being refreshed to identify and mitigate horizontal issues more easily across programs.

[12] Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks Guidelines, Treasury Board, April 2012.

The Department has implemented a new methodology in 2014 for the prioritization of PIAs. The methodology tracks departmental PIA priorities and includes risk levels, time sensitivities and the status of individual PIAs. This approach is intended to provide more useful information to PISC members about the status of PIAs and to better allow enabling branches to strategically dedicate resources to the development of priority PIAs.

Recommendation 3

IITB, in partnership with the Corporate Secretary, in her capacity as CPO, should ensure that approaches to the PIA, SA&A and TRA processes are better aligned and integrated to provide a comprehensive view of privacy and security risks (physical and IT) in a consistent and timely manner.

Management Response

The ADM of IITB and the Corporate Secretary, in her capacity as CPO, concur with the recommendation. IITB has completed the integration of TRAs into the SA&A process. Enhancing the alignment of the SA&A and PIA processes will be completed by summer 2015.

2.5 Assurance of Compliance

The Department uses various mechanisms to monitor the Framework for the management of personal information

Overall, the Department has taken multiple approaches to monitor its Privacy Framework. As mentioned earlier in this report, having a dedicated and functioning governance structure through bodies such as PISC and CMC and dedicated positions like the CPO ensure that privacy remains on the management agenda. In addition, ESDC was also subjected to external and internal audits which highlighted areas for improvement. Action plans to address the gaps have been developed and are being implemented. Lastly, the Office of Values and Ethics reports on incidents involving the Code of Conduct and as such some of these incidents may involve privacy or security.

At the program level, PLPAPs have identified a number of priority areas that are common across programs. A risk assessment refresh is underway to triage the PLPAPs horizontally to allow for easier monitoring.

The Department is monitoring systems for incidents and access controls. All employee computers are being monitored for non-sanctioned USBs being plugged into the network. IITB has also conducted scans of outgoing emails and sample phishing attacks. The DSO has implemented security sweeps in NHQ, and the audit team was also informed that security sweeps will be implemented in the regions in fiscal year 2015–2016. In regards to access controls, programs stated through interviews that there is an opportunity to strengthen monitoring of employee access to the various systems. They provided examples of employees who have left the Department or have moved within the Department that have not had their access rights to ESDC systems revoked. Weaknesses pertaining to the monitoring of access have been raised in previous audits. Action plans have been developed and are being implemented to address the gaps that have been identified.

3.0 Conclusion

The audit concluded that ESDC's PMF is adequate to address most privacy-related concerns. There are processes and controls in place that are sustainable over time, including a dedicated governance body and a policy suite for privacy management. However, there are still areas of the PMF that could be improved. Opportunities exist to further integrate the PIA, SA&A and TRA processes, to institute consolidated privacy incident trend reporting, and to improve the stewardship of ISAs.

4.0 Statement of Assurance

In our professional judgement, sufficient and appropriate audit procedures were performed and evidence gathered to support the accuracy of the conclusions reached and contained in this report. The conclusions were based on observations and analyses at the time of our audit. The evidence was gathered in accordance with the Internal Auditing Standards for the Government of Canada and the International Standards for the Professional Practice of Internal Auditing.

Appendix A: Audit Criteria Assessment

Control Component	Audit Criteria It is expected that:	Rating
Governance and Accountability	The Department's governance structure clearly addresses privacy management.	●
	The Department defines, documents, communicates and assigns accountability for its privacy policy and procedures.	●
	Privacy policies and procedures are reviewed and compared to the requirements of applicable laws and regulations.	✪
Stewardship of Personal Information	The control framework to protect the personal information throughout the life-cycle of the information is defined, documented and complies with the *Privacy Act,* R.S.C. 1985, c. P-21 and the *Department of Employment and Social Development Act*.	●
	Privacy policies and the consequences of noncompliance with such policies are communicated to the Department's personnel responsible for collecting, using, retaining, and disclosing personal information.	●
	The types of personal and sensitive information and the related processes, systems, and third parties involved in the handling of such information are identified. Such information is covered by the Department's privacy and related security policies and procedures.	◘
	A documented privacy incident and breach management program has been implemented.	◘
Culture, Awareness and Training	A privacy awareness program is in place, and training for selected personnel depending on their roles and responsibilities, is provided.	●
	The Department has an established Code of Conduct that addresses expectations for the protection of personal information.	●
Risk Management	A risk assessment process is used to establish a risk baseline, to identify and assess new or changed risks to personal information, and to develop and update responses to such risks.	◘
	Management measures and reports on its performance against defined expectations for privacy management.	●
Assurance of Compliance	The Department monitors compliance with its privacy policies and procedures and has procedures to address privacy-related inquiries, complaints and disputes.	●

✪ = Best practice
● = Sufficiently controlled, low risk exposure
◘ = Controlled, but should be strengthened, medium risk exposure
○ = Missing key controls, high risk exposure

Appendix B: Glossary

ADM	Assistant Deputy Minister
CMC	Corporate Management Committee
CPO	Chief Privacy Officer
CRP	Corporate Risk Profile
DESD	Department of Employment and Social Development
DM	Deputy Minister
DPPM	Departmental Policy on Privacy Management
DSO	Departmental Security Officer
ESDC	Employment and Social Development Canada
IITB	Innovation, Information, and Technology Branch
IM	Information Management
ISA	Information Sharing Agreement
IT	Information Technology
NHQ	National Headquarters
PIA	Privacy Impact Assessment
PISC	Privacy and Information Security Committee
PLPAP	Program-led Privacy Action Plans
PMF	Privacy Management Framework
SA&A	Security Assessment and Authorization
SIMU	Security Incident Management Unit
SIWB	Stewardship of Information and Workplace Behaviours
TRA	Threat and Risk Assessment