Protected B

HUMAN RESOURCES AND SKILLS DEVELOPMENT CANADA

Departmental Security Plan

2012 – 2015

Date: June 21, 2012

Internal Integrity and Security Directorate
Integrity Services Branch

NOT FOR DISTRIBUTION

Protected B

Message from the Deputy Minister

I am pleased to publish the Departmental Security Plan, as required by the Treasury Board *Directive on Departmental Security Management* under the authority of the *Policy on Government Security*. The Departmental Security Plan sets out the plans, priorities and requirements for Human Resources and Skills Development Canada regarding the design, implementation and maintenance of its Security Program.

Effective security management is key to the safety of the personnel of Human Resource Skills Development Canada (HRSDC) and to the integrity of HRSDC information, assets and services. Security supports and enables the achievement of the department's business objectives. It is therefore essential that HRSDC personnel involved in the security management function and all managers ensure that all staff understands their security responsibilities.

The HRSDC Departmental Security Plan is the responsibility of the Director General, Internal Integrity and Security, and Departmental Security Officer, to whom all comments and questions should be directed. Revisions and updates will be issued as often as necessary to keep this Plan current.

Ian Shugart
[Signature]

Deputy Minister, Human Resources and Skills Development Canada

[Date]

Protected B

Table of Contents

MESSAGE FROM THE DEPUTY MINISTER II

TABLE OF CONTENTS III

ACRONYMS V

EXECUTIVE SUMMARY VI

1 DEPARTMENTAL CONTEXT 1

1.1 MISSION AND MANDATE 1

1.2 STRATEGIC OUTCOMES AND PRIORITIES 1

1.3 AUTHORITIES 2

2 DEPARTMENTAL SECURITY CONTEXT 3

2.1 SECURITY AS AN ENABLER 3

2.2 SECURITY GOVERNANCE 4

2.2.1 Security Integration 4

2.2.2 External Liaison 5

2.3 SECURITY PROGRAM FUNCTIONS 5

2.3.1 Corporate Security and Internal Integrity Division 6

2.3.2 Emergency Management and Business Continuity (EMBC) 7

2.3.3 Office of Values and Ethics 8

2.3.4 IT Security Centre of Excellence – Innovation, Information and Technology Branch 8

2.3.5 Regional Internal Integrity and Security 9

3 HRSDC DEPARTMENTAL SECURITY PLAN 11

3.1 OBJECTIVE 11

3.2 SCOPE 11

3.3 DEVELOPMENT PROCESS 11

4 SECURITY RISK MANAGEMENT 13

4.1 CORPORATE RISK MANAGEMENT 13

4.2 SECURITY RISK AREAS 14

4.2.1 Security Risk Area 1: Information Assurance 14

4.2.2 Security Risk Area 2: Individual Security Screening 15

4.2.3 Security Risk Area 3: Physical Security and Access Control 16

4.2.4 Security Risk Area 4: IT Security 17

4.2.5 Security Risk Area 5: Incident Management, Emergency Management and Business Continuity 18

4.2.6 Overarching activities 19

4.2.7 Controls to manage Security Risk Areas 21

1. Overarching activities 21
2. Security Risk Area 1: Information Assurance 22
3. Security Risk Area 2: Individual Security Screening 23
4. Security Risk Area 3: Physical Security and Access Control 23
5. Security Risk Area 4: IT Security 24
6. Security Risk Area 5: Incident Management, Emergency Management and Business Continuity 26

5 IMPLEMENTATION, MEASUREMENT, REPORTING AND UPDATE 28
5.1 IMPLEMENTATION PLAN 28
5.2 PERFORMANCE MEASUREMENT STRATEGY FRAMEWORK 28
5.3 REPORTING 29
5.4 REVIEW AND UPDATE 31
6 BUILDING CAPACITY AND MATURITY 32
APPENDIX A: DSP IMPLEMENTATION PLAN 33
APPENDIX B: LOGIC MODEL 44
APPENDIX C: MATURITY MODEL 45

Acronyms

CFOB	Chief Financial Officer Branch
CPP	Canada Pension Plan
CSLG	Canada Student Loans and Grants
DDSM	Directive on Departmental Security Management
EI	Employment Insurance
ICMS	Incident Case Management System
IITB	Innovation, Information and Technology Branch
IISD	Internal Integrity and Security Directorate (HRSDC)
InSNC	In-Person Integrity Services National Committee (HRSDC)
ISB	Integrity Services Branch (HRSDC)
IT	Information Technology
ITSCOE	Information Technology Security Centre of Excellence
NCR	National Capital Region
NIISC	National Internal Integrity and Security Committee (HRSDC)
OAS	Old Age Security
PGS	Policy on Government Security
RDM	Resource Determination Model
SRCL	Security Requirements Check List
SSC	Shared Services Canada

Protected B

Executive Summary

The 2009 Treasury Board *Policy on Government Security* (PGS) emphasizes the need for sound security governance, accountability and management. In that regard, the Policy requires departments to develop a long-term security plan to sustain a strong culture of security and to enable security teams to manage daily security operations.

The Human Resources and Skills Development Canada (HRSDC) Departmental Security Plan (DSP) is the vehicle to ensure that the PGS requirements are met. The HRSDC DSP is based on key security risk areas that are unique to the Department because of its mandate and strategic outcomes. For each of these risk areas listed below, the DSP describes the required components to mitigate these risks for the delivery of an effective security program:

- Information Assurance: Information security, personal information protection and effective stewardship of information and assets;
- Individual Security Screening: Trustworthy and reliable staff who understand their security responsibilities – employees, contractors, students and all other individuals who have access to HSRDC resources;
- Physical Security and Access Control: Physical security and access control for the protection of staff and clients, service delivery, information and assets;
- IT Security: Information Technology (IT) systems and network protection; and
- Incident management, Emergency Management and Business Continuity: Incident management to protect employees and clients, and to support the continued availability of services in emergency and crisis situations.

The DSP is aligned with the HRSDC corporate risk management approach. This approach meets the PGS requirements to integrate security planning, priorities and performance with departmental business plans and priorities.

This plan includes a multi-year plan for an improved security program by defining existing controls, gaps and additional controls that should be put in place.

In addition, the DSP will continue to be updated regularly, as security risks change over time, with new risks arising and existing risks addressed through new or adjusted security controls.

1 Departmental Context

1.1 Mission and Mandate

The mission of Human Resources and Skills Development Canada (HRSDC) is to build a stronger, more competitive Canada, to support Canadians in making choices that help them lead productive and rewarding lives, and to improve Canadians' quality of life.

HRSDC is responsible for designing and delivering some of the Government of Canada's most well-known statutory programs and services, including:

- Old Age Security (OAS);
- Canada Pension Plan (CPP);
- Employment Insurance (EI);
- Canada Student Loans and Grants (CSLG);
- National Child Benefit;
- Universal Child Care Benefit.

These direct benefits to Canadians are part of Canada's social safety net and represent almost 95 percent of the Department's expenditures.

Service Canada helps citizens access HRSDC's programs, as well as other Government of Canada programs and services, online at www.servicecanada.gc.ca, by telephone through 1 800 O-Canada, and at more than 600 points of service across the country through its network of program-based call centres. In 2012-2013, HRSDC will continue to play a key role in delivering programs and services for citizens and employers as they adapt to changing economic conditions and prepare for the future.

Through the Labour Program, the Department is responsible for overseeing federal labour responsibilities, including labour laws; occupational health and safety; labour standards; labour relations and mediation services in federally regulated workplaces. The Labour Program also represents Canada in international labour organizations and negotiates labour cooperation agreements as part of free-trade negotiations.

Finally, grants and contributions funding is provided to other levels of government and organizations to support projects that meet the labour market and social development needs of Canadians.

1.2 Strategic Outcomes and Priorities

The HRSDC Security Program is critical in supporting the Department's four strategic outcomes:

- A skilled, adaptable and inclusive labour force and an efficient labour market
- Safe, fair and productive workplaces and cooperative workplace relations
- Income security, access to opportunities and wellbeing for individuals, families and communities
- Service excellence for Canadians

In the HRSDC Program Activity Architecture, the Internal Services element supports the achievement of the Department's strategic outcomes by providing the resources, guidance, support services and information necessary to design and deliver programs and services. This element includes specifically the Security Program, which is managed by the Internal Integrity and Security Directorate.

The HRSDC Security Program provides security services to the portfolio to achieve excellence in delivering programs and services to Canadians with a coordinated and integrated security program that is aligned with government-wide security requirements. The underlying foundation of security activities – protecting employees, information and assets, and ensuring the continuity of government operations and services – is important to achieving the HRSDC mission.

1.3 Authorities

Human Resources and Skills Development Canada is governed by two main acts:

- *Department of Human Resources and Skills Development Act* and
- *Department of Social Development Act*.

Authority for the DSP also derives from the following legislation, policies and departmental management instruments:

- HSRDC Integrated Business Plan (2010-2013)
- HRSDC Report on Plans and Priorities (2011-2012)
- HRSDC Departmental Performance Report (2009-2010)
- HRSDC Departmental Strategic Emergency Management Plan (2012)
- HRSDC Policy on Departmental IT Security Management (2009)
- HRSDC Code of Conduct
- *Access to Information Act*
- *Canada Pension Plans Act*
- *Emergency Management Act*
- *Employment Insurance Act*
- *Financial Administration Act*
- *Labour Adjustment Benefits Act*
- *National Housing Act*

- *Privacy Act*
- *Security of Information Act*
- Canada Labour Code - Part I, Industrial Relations and Part II, Occupational Health and Safety
- Criminal Code
- Treasury Board Policy on Government Security (2009)
- Treasury Board Directive on Departmental Security Management (2009)
- Treasury Board Fire Safety Standard (2010)
- Treasury Board Standard for Fire Safety Planning and Fire Emergency Organization, Chapter 3-1

2 Departmental Security Context

2.1 Security as an Enabler

Given the nature of HRSDC and its services and programs, the Department needs a strong security structure. The volume and sensitivity of information, including personal and identity information of Canadians, the number of Service Canada offices and processing centres and their widespread geographic locations, combined with the mandate for multiple and accessible service delivery channels present a unique security challenge.

This challenge is most evident in Service Canada Centres (SCC). SCCs are located in public places such as shopping malls and in facilities often shared with other tenants. These centres have equipment, systems and documents with personal information, as well as employees who serve clients, requiring robust security protection.

Continuous assessment of threats, vulnerabilities and risks to the achievement of objectives, combined with careful planning, implementation, quality assurance and review of security controls are an integral way of doing business that enables service delivery across the country.

HRSDC program and business areas are responsible for integrating the necessary security controls to protect individuals, information, assets and services during normal operations, and when developing more efficient external and internal services. Internal service initiatives include:

- EI automation;
- CPP and OAS Modernization;
- pursuing higher levels of self-service and online transactions;
- Enabling Services Renewal Program (ESRP); and
- expanding service delivery on behalf of other federal departments.

External initiatives that impact security include:

- Deficit-Reduction Action Plan (DRAP);
- transitioning IT to Shared Services Canada (SSC);
- upcoming changes to individual security screening requirements by TBS; and
- Administrative Services Renewal.

2.2 Security Governance

HRSDC has made significant progress over the past years in instilling a culture of security throughout the Department: executives, managers and staff have a better understanding of the rationale of security, its support to achieving business objectives, and their own roles and responsibilities with respect to security.

This effort must be continued and enhanced. This DSP outlines what can be done to innovate and improve on existing practices to enhance the HRSDC security culture.

2.2.1 Security Integration

As required by the PGS, HRSDC has integrated security domains into one point of accountability, the Departmental Security Officer (DSO). The Deputy Minister, accountable for security governance and management, has delegated the ongoing management of the departmental Security Program to the DSO. At HRSDC, the DSO is the Director General of the Internal Integrity and Security Directorate (IISD), Integrity Services Branch (ISB).

The reporting structure, that includes both direct and functional reporting to the DSO, ensures that security program management is consistent throughout the Department. Regional Executive Directors of Integrity (REDs) report functionally to the DSO on security matters and are responsible for managing the Security Program within their Regions, in consultation with the DSO. Regional Internal Integrity and Security (Regional IIS) Operations manage and operate all aspects of security and emergency management in their Regions.

The Information Technology (IT) Security Program is governed under the leadership of the Chief Information Officer (CIO) as per the Policy on Departmental IT Security Management (DITS Pol). The Director of the Information Technology Security Centre of Excellence (ITSCOE), who is also the Departmental IT Security Coordinator (DITSEC), reports functionally to the DSO.

The Security Program governance structure enables effective collaboration at each level of security, both nationally and regionally, including the National Internal Integrity and Security Committee (NIISC) involving NHQ and the Regions, and through participation at corporate committees such as the Corporate Management Committee (CMC), the Legal

Issues Management Committee (LIMC) and the Privacy and IT Security Committee (PISC), as well as regional executive committees. There is a strong working relationship with key related functions: Legal Services, Human Resources Services Branch (HRSB), Innovation and Information Technology Branch (IITB), Access to Information and Privacy (ATIP) and the Service Canada College.

The Department has established a departmental Crisis Management Team (CMT), chaired by the Senior Associate Deputy Minister of HRSDC and Chief Operating Officer (COO) for Service Canada. The CMT leads departmental emergency response, business continuity and incident recovery activities and related critical decision-making.

2.2.2 External Liaison

IISD/ISB and ITSCOE/IITB work collaboratively with other government departments within the service delivery portfolio and with those that share service delivery programs, notably the Canada Revenue Agency and Passport Canada.

The Directorates also respond to the leadership of the central and lead security agencies:

- Treasury Board Secretariat (TBS): lead for overall government security policy, including business continuity planning policy instruments and government-wide collaboration in security;
- Public Safety Canada (PSC): lead for emergency management and information interoperability. HRSDC works with Public Safety Canada in view of its leadership role under the *Emergency Management Act*, Federal Emergency Response Plan (FERP), and for the management of the Department's National Emergency Operations Center (NEOC);
- Canadian Security and Intelligence Service (CSIS): lead for individual security screening for access to classified information;
- Royal Canadian Mountain Police (RCMP): lead for physical security and protective services for Ministers' Offices;
- Communications Security Establishment Canada (CSEC): lead for electronic information and communication (IT security), and
- Public Works and Government Services Canada (PWGSC): lead for security and IT security in contracting.

The Security Program also works closely with police organizations across all regions that provide law enforcement and criminal investigation services.

2.3 Security Program Functions

The HRSDC Security Program, which is administered by IISD, provides security services to all programs and services across the Department's portfolio both at National Headquarters

(NHQ), including Region 5 National Capital Region (NCR), and across the four other Regions: Atlantic, Quebec, Ontario and the Western Canada and Territories Region.

At NHQ, the HRSDC Security Program has three divisions that report to the DSO:

- Corporate Security and Internal Integrity,
- Emergency Management and Business Continuity, and
- Office of Values and Ethics.

2.3.1 Corporate Security and Internal Integrity Division

The activities of the Corporate Security and Internal Integrity division include:

- Security training and awareness: security training of staff; security awareness sessions; notifications; alerts and bulletins; and the Security Program Intranet site;
- Security advice on provincial and territorial information sharing agreements (ISAs) and support of these ISAs;
- Oversight of security requirements for contracts and cross references pertaining to these requirements;
- Development and implementation of Corporate Security policies, directives, guidelines, and manuals;
- Individual security screening: Reliability status for all staff, students, Ministerial staff, etc. and security clearances, as required; regular updates, and as warranted by changes in position descriptions;
- Development and implementation of Threats and Risks Assessments; (TRAs)
- Communications security: special protection of cryptographic materials, installation and maintenance of secure phones and faxes;
- Physical security, including all aspects of physical access control; security planning in site/facility selection and refit; and environmental protection;
- Protection of employees in the workplace;
- Response to, resolution of and reporting on security incidents and privacy breaches;
- Functional advice, guidance and support to the Regional IIS units; and
- Alternate Deputy DSO.

The Corporate Security and Internal Integrity division is also responsible for managing all aspects of security in the National Capital Region (NCR) (Region 5), including ensuring the security of ministers, deputy ministers, and managing the VIP Protective Services.

The Special Investigations Unit (SIU) conducts administrative investigations of suspected, alleged and actual wrongdoing, and coordinates with law enforcement agencies for potentially criminal misconduct. As required, Regional IIS Operations conduct their own investigations and/or assist the SIU with their work.

2.3.2 Emergency Management and Business Continuity (EMBC)

ISSD is responsible for leading the development of an integrated and coordinated approach for all emergency management and business continuity activities across the portfolio including preparedness and response activities, the development of tools, plans and communications required to ensure individual and overall departmental readiness in the event of an emergency. The directorate leads all departmental Building Emergency Organization activities including preparedness and response activities related to evacuations and all required training and awareness of emergency teams to ensure a safe evacuation in the event of an emergency situation. The department has developed the Departmental Strategic Emergency Management Plan (SEMP), the Departmental Business Continuity Management Program (BCMP), and business continuity plans (BCPs) for all HRSDC facilities,

Leadership and assistance are provided to programs to develop their business continuity plans in order to support the continued delivery of services to Canadians or to minimize the impact on services for staff, clients and partners during events such as postal strikes, bomb threats, building occupation by demonstrators, as well as natural events, such as pandemic illnesses, fires, floods, and earthquakes.

In addition to maintaining continued delivery of services to Canadians, HRSDC is the primary department under the *Federal Emergency Response Plan* (FERP) for Emergency Support Function (ESF) 7 – *Human and Social Services*.

Furthermore, IISD provides government-wide support under the following emergency support functions:

- ESF 5 – *Public Health and Essential Human Services* (led by Health Canada and Public Health Agency of Canada);
- ESF 11 – *Logistics Operations Management* (led by Public Safety); and
- ESF 12 – *Communications* (led by Public Safety).

IISD also operates the National Emergency Operations Centre (NEOC), which is supported by Regional Emergency Operations Centres (REOCs); the NEOC is also the primary back-up site to the Government Operations Centre managed by Public Safety Canada.

To align with the Government of Canada's *FERP* and in accordance with the *Emergency Management Framework for Canada* and the *Federal Policy for Emergency Management*, HRSDC uses an all-hazards approach to emergency management.

2.3.3 Office of Values and Ethics

The Office of Values and Ethics acts as a centre of expertise for Public Service values and ethics, with the purpose of fostering, sustaining and promoting the ethical, honest and principled behaviour of employees. As such, the Office also plays an oversight role across the Department, using among other things, the new HRSDC Code of Conduct launched in April 2012. The Office supports the Senior Disclosure Officer – the Assistant Deputy Minister of the Integrity Services Branch (ISB) - in implementing the *Public Servants Disclosure Protection Act* (PSDPA) within HRSDC and the Canada Employment Insurance Commission.

The activities of the Office of Values and Ethics include:

- Implementing the *Public Servants Disclosure Protection Act* in HRSDC;
- Receiving and responding to enquiries related to the HRSDC Code of Conduct, values and ethics, conflict of interest and disclosure of wrongdoing;
- Managing cases related to breaches of the HRSDC Code of Conduct, including breaches related to values and ethics, conflict of interest and the *Public Servants Disclosure Protection Act*;
- Providing values and ethics guidance, advice, training and awareness to employees, managers and executives;
- Oversight on conflict of interest measures within HRSDC's Interchange Canada Program;
- Functional advice, guidance and support to Regions;
- Reporting to Treasury Board Secretariat annually on the Department's performance in the area of Values and Ethics as part of the Management Accountability Framework (MAF) initiative, and all activities related to the *Public Servants Disclosure Protection Act*.

2.3.4 IT Security Centre of Excellence – Innovation, Information and Technology Branch

The IT Security Program is led by the Chief Information Officer (CIO) and Departmental IT Security Coordinator (DITSEC) under the Policy on Departmental IT Security Management (DITS Pol). The management of IT security is a mandatory enabler of HRSDC's management practices and GC's ability to deliver IT security services to HRSDC programs and services to all Canadians in an ever-evolving environment.

ITSCOE is responsible for managing safeguards to preserve the confidentiality, integrity, privacy, availability, intended use and value of electronically stored, processed or transmitted information. It is also responsible for the IT assets used to gather, process, receive, display, transmit, reconfigure, scan, store or destroy information electronically.

ITSCOE also works with the DSO when IT security incidents have an impact on areas of security other than IT.

ITSCOE is organized into streams of functions at the departmental level as follows:

- IT Security Accreditation Program;
- IT Security Architecture;
- IT Security Program Management and Coordination;
- IT Security Awareness Program; and
- IT Security Business Continuity Planning.

With the announcement of the new Shared Services Canada (SSC) in late 2011, the specifics with respect to security responsibilities are still being clarified. SSC is responsible for providing its partner organizations with modern, reliable and secure IT infrastructure services.

2.3.5 Regional Internal Integrity and Security

Consistency across HRSDC is assured through the integrated model now in place, and with the Regional Executive Directors (REDs) reporting functionally to the DSO on security- and integrity-related matters, including incidents occurring in the Regions. Regional IIS Operations encompass all areas of security, including emergency management.

The Regional Managers (RMs), who report to the REDs in the regions and to the Director of Corporate Security and Internal Integrity for NCR (Region 5), manage security and emergency management and business continuity functions, including:

- Training and awareness
- Personnel security screening
- Physical security
- Communication security
- Security incidents
- Investigations
- Emergency management and business continuity planning

The RMs develop and implement the Region Security Plan, which mirrors and achieves the goals and commitments of the DSP, and they implement the PGS within their designated Regions. The RMs also contribute to national program and policy development. Moreover, they develop and implement regional guidelines and strategies for security business continuity and emergency preparedness, assuring consistency with the overall security program.

Region	# of Sites	Employees (approx.)
Atlantic	88	2,600
Quebec	117	3,300
Ontario	198	4,800
West & Territories	222	4,900
NCR Region	28	7,500
TOTAL	**653**	**23,100**

Table: HRSDC regional breakdown of sites and of number of employees (as of March 31, 2012)

3 HRSDC Departmental Security Plan

3.1 Objective

The objective of the HRSDC DSP is to detail plans for managing security risks and to outline objectives, controls, accountabilities and timelines for continuous improvement of security at HRSDC.

The DSP seeks to provide to the Deputy Minister and Corporate Management Committee (CMC) an integrated view of security requirements, aligned with HRSDC strategic priorities, plans and program activities. The outcome will be a security program focused on the highest priority security risks to achieve the Department's Strategic Outcomes.

Without a cohesive, long-term plan, continuous improvement of security at HRSDC is difficult to achieve while managing daily operational activities. Therefore, the DSP aims to assist in achieving the objectives of daily operational management to address the current threat environment, to plan for anticipated trends in threats and risks within the departmental context, and to comply with legislation, policy and central agency requirements.

3.2 Scope

The DSP covers the design, implementation and maintenance of all aspects of security for all of HRSDC while reflecting HRSDC-specific priorities and plans. Based on the PGS, the scope of the HRSDC DSP covers all security functions of the Department including those functions whose management intersect with security. This includes access to information, privacy, risk management, emergency and business continuity management, human resources, occupational health and safety, real property, materiel management, information management, information technology (IT) and finance.

3.3 Development Process

The PGS requires the DM to approve a DSP that details plans for managing security risks and outlines objectives, priorities, accountabilities and timelines for improving departmental security and supporting the implementation of the DSP.

The departmental lead for the development and the implementation of the Plan is the Departmental Security Officer (DSO), Director General of the Internal Integrity and Security Directorate, at the Integrity Services Branch.

A DG-level working group on the DSP was formed in 2010 and meets as needed to reflect all branches' assessments of their own security risks and to define the optimal mitigation strategies.

Under the leadership of the DSO, the Department has initiated the identification and assessment of security risks. This exercise will be completed in the upcoming months. The resulting plan will be periodically revisited by the DSP Working Group to ensure a continual update, to adapt the plan to changing circumstances and to further guide the development of various elements and controls that are required to fully implement it.

4 Security Risk Management

Under the PGS, the departmental Security Program must be risk-based. The *Guideline on the Development of the Departmental Security Plan* establishes the security risk management premise of the DSP and describes the methodology.

4.1 Corporate Risk Management

Integrated risk management at HRSDC is a structured, systematic approach to identifying, assessing and managing risk. It assists the Department in anticipating potential problems and taking steps to address them before they occur to allow the Department to continue to meet its goals despite changes in its external or internal environment.

The objectives of HRSDC's Corporate Risk Profile are to establish a shared understanding at the senior level of the most significant risks to the Department's ability to achieve its Strategic Outcomes over the next three to five years, and to establish a basis to proactively manage those risks.

The Department has identified the following Corporate Risks for 2012-2013. Security is a component of the mitigating strategies that are identified for all of these four risks:

- Transformation Agenda
- Privacy
- Information Technology
- Human Resource Management

- **Transformation Agenda**

HRSDC is undertaking a significant transformation agenda with several large, complex, horizontal change initiatives. This agenda includes several internal business transformation initiatives, which require the delivery of multiple, competing and interdependent projects by enabling services branches, including the Security Program.

- **Privacy**

Privacy protection is critical to maintain Canadians' trust—an essential precursor to their willingness to share information and make electronic transactions. To help ensure the protection of personal information and respect for the privacy of Canadians, HRSDC will continue to strengthen its privacy management and assurance.

- **Information Technology**

The Department invests in information technology (IT) business applications on an ongoing basis, continuously replacing obsolete or inadequate software and acquiring new technologies, as required. Going forward, HRSDC will need to continue positioning its

investments within the broader context of its priorities and plan appropriately for ongoing maintenance. HRSDC will align software with government-wide services (such as Shared Services Canada) and standards that include security requirements.

- **Human Resource Management**

A greater focus on multi-year integrated business planning, supported by an effective workforce management strategy, will allow the Department to have the right people in the right place at the right time. HRSDC will adopt a national learning strategy and seek new learning technologies to support its employees, as well as a leadership strategy to give leaders tools to help them create and sustain a healthy and enabling workplace.

4.2 Security Risk Areas

The DSO has started developing a risk assessment to align with the HRSDC Corporate Risk Management Framework process and to align with the TBS security risk management process, as set out in the TBS *Guideline on the Development of a Departmental Security Plan*. In compliance with these requirements and in line with corporate risk management practices, over the past 18 months, IISD conducted a risk identification session (December 2010) and a risk assessment workshop (March 2011). The identified risks were then rolled up in 5 strategic risk areas, providing the Department with a sharper focus of its priorities. The risk assessment exercise will continue to ensure that emerging or changing risks are identified and addressed.

Preliminary work in risk management has identified the following five security risk areas:

 # 1: Information Assurance
 # 2: Individual Security Screening
 # 3: Physical Security and Access Control
 # 4: IT Security
 # 5: Incident management, Emergency Management and Business Continuity

For each risk areas, the following elements were identified and are listed in this section:

- Objective
- Threats
- Vulnerabilities

4.2.1 Security Risk Area 1: Information Assurance

HRSDC conducts a high volume of financial transactions with clients and other departments. In the federal government, HRSDC is the custodian of the most detailed and complete set of records and, as such, has numerous systems in place to protect the

personal information databases that the Department manages. Privacy protection is critical and to this end, the federal *Privacy Act* includes a code of fair practices concerning the collection, use, disclosure, retention and disposal of personal information. In addition, the set of Privacy Codes contained within the Department's enabling legislation imposes rules for information use and availability that exceed Privacy Act requirements, with significant penalties for the misuse of personal information.

To help ensure the protection of personal information and respect for the privacy of Canadians, HRSDC will continue to strengthen its privacy management and assurance. Robust mitigation of this risk area is ongoing, including awareness and training strategies, as well as continued implementation of the Department's Privacy Management Framework.

Objective: *Ensure the effectiveness of information management practices and equipment to ensure the confidentiality, integrity, privacy and availability of information.*

Threats:	**Vulnerabilities:**
• Human error • Cyber attacks • Network intrusions • Employee wrongdoing or negligence • Criminal activities (break-and-enter, financial or identity fraud and theft, vandalism) • Modification or destruction of data • Natural hazards (flood, fire, weather events)	• Lack of employees' awareness on: – Information and asset identification and categorization (sensitivity); – Security responsibilities (managers and staff) • Outdated policies, standards and procedures • Inadequate IT training (software/network errors) • Aging IT infrastructure • Weak IT and physical access controls

4.2.2 Security Risk Area 2: Individual Security Screening

Ensuring that all individuals who have access to government information and assets are security screened at the appropriate level before they start their duties and throughout their tenure is a key component of the security program of all federal institutions.

Security screening requirements apply to contractors and employees. PWGSC is responsible for the security screening of contractors doing business with the Government of Canada.

A Reliability Status or security clearance is intended to provide assurance that the identities of individuals are verified to the extent required, and that all individuals who work for the Department are reliable, honest, trustworthy and, with respect to security clearance, loyal to Canada. The PGS baseline security screening requirement for access to government facilities, information and assets is Reliability Status (RS). Through jurisprudence, RS is now a condition of employment.

Approximately 90% of HRSDC employees have RS, and the other 10% have security clearances mostly at Level II (Secret), and a small number at Level III (Top Secret).

Objective: *Ensure that all employees, contractors and ministerial personnel are security screened, based on their current position descriptions or contract statements of work, and that the security status is reassessed, based on changing work descriptions or other factors, including individuals' behaviours or actions that may lead to suspicion of wrongdoing.*

Threats:

- Dishonest or untrustworthy individuals will lead to compromise, fraud, or identity theft

Vulnerabilities:

- Unreliable employees may make mistakes or be negligent, leading to compromise
- Inadequate controls to ascertain accuracy of security clearance level with respect to the position of incumbents
- Security screening of contractors is done by another department

4.2.3 Security Risk Area 3: Physical Security and Access Control

Given its 600 and more points of service, office locations in a wide variety of physical spaces (including co-locations with both public and private sector organizations) and the public-facing nature of most locations, there are increased risks of employee injury by angry clients or other disgruntled individuals, unauthorized access to sensitive information and building security zones, and interruption of critical services.

Ensuring adequate physical access control and physical security measures for the protection of information, assets and employees is essential for the success of the security program.

Objective: *Ensure the effectiveness of physical security controls throughout the*

Department, regardless of location, through robust physical control practices, measures, regular monitoring and inspections.

Threats:

- Employee wrongdoing or negligence
- Disaffected clients
- Criminal activities (break-and-enter, financial or identity fraud, theft and vandalism)
- Natural hazards (flood, fire, weather events)

Vulnerabilities:

- Lack or inadequacy of robust physical controls, including regular monitoring and inspections
- Lack of employee awareness on threats and the importance of controls
- Inadequate implementation of policies, standards and procedures (e.g., interior design security requirements)

4.2.4 Security Risk Area 4: IT Security

HRSDC relies on the integrity, reliability and availability of its IT systems. The sheer volume of IT systems and electronic financial and personal transactions makes HRSDC systems prime targets for attack, leading to compromise. The Department would be vulnerable if it did not have sufficiently robust IT access controls as well as strong employee awareness of the threats and vigilance in counteracting such threats.

IITB is currently in the process of finalizing the IITB Risk Management Policy, which establishes continuous risk management processes, such as vulnerability analyses, IT service continuity management and internal audits (clarify respective roles of HRSDC and SSC).

***Objectives**: Counter threats, vulnerabilities and unauthorized access to the Department's systems to ensure and protect the confidentiality, integrity, privacy and availability of all departmental information such as client, employee, and other sensitive information. Ensure that the required IT infrastructure is in place to prevent any service interruptions to mission-critical functions.*

Threats:

- Cyber attacks
- Network intrusions
- Criminal activities
- Natural hazards (flood, fire, weather events)

Vulnerabilities:

- High volume of electronic financial and personal transactions, which makes HRSDC prime targets for attack
- Lack of employees awareness on threats and vigilance in counteracting such

threats
- Inadequate training (IT, software/network errors; security)
- Aging IT infrastructure
- Weak IT controls

4.2.5 Security Risk Area 5: Incident Management, Emergency Management and Business Continuity

Given its size and scope, HRSDC is attractive to attackers, which increases the likelihood of security incidents, privacy breaches and service interruptions. Also, the large number of staff and variety of locations across Canada create more opportunity for accidental compromise.

Security Incidents include threats against employees, facilities and third parties; threats of suicide; vandalism; break-ins; theft of assets, information and negotiable; physical assaults; and loss of departmental assets including access cards or photo identification. Each of these incidents is managed at the regional level and reported to NHQ.

In the event of a wide-scale emergency, the Department is responsible for maintaining key and critical services and benefits to Canadians, communications, as well as regulatory services on labour standards, with minimum disruption for the public.

In addition to maintaining continued delivery of services to Canadians, HRSDC is the primary department under the *Federal Emergency Response Plan* (FERP) for Emergency Support Function (ESF) 7 – *Human and Social Services*. Under *ESF 7*, the Department maintains continued delivery of financial compensation, social benefits and access to key programs and services with minimal disruption. HRSDC also supports the needs of municipalities, provinces, territories and federal institutions with an array of services, assets and infrastructure that may assist in responding to an emergency or crisis situation.

The Department also has the responsibility to maintain a back-up site for the Government Operations Centre. Public Safety relies on the HRSDC National Emergency Operations Centre as the primary back-up for the Government Operations Centre.

As well, HRSDC provides support to other federal institutions under the following emergency support functions:
- ESF 5 – *Public Health and Essential Human Services* (led by Health Canada and Public Health Agency of Canada);
- ESF 11 – *Logistics Operations Management* (led by Public Safety); and
- ESF 12 – *Communications* (led by Public Safety).

Objective: Mitigate security and emergency incidents by:

- being prepared to identify threats with the potential to cause incidents;
- countering threats before incidents occur; and
- responding to incidents by preventing or minimizing effects and potential losses, and by supporting the continued delivery of critical services.

Threats:

- Human error
- Employee wrong-doing or negligence
- Disaffected client
- Protests and demonstrations
- Criminal activities (break-and-enter, financial or identity fraud and theft, vandalism)
- Cyber attacks
- Network intrusions
- Natural hazards (flood, fire, weather events)

Vulnerabilities:

- Lack of employees awareness on security and emergency incident management
- Lack or inadequacy of inspections and exercises
- Inadequate implementation of policies, standards and procedures (e.g., prevention, detection, response to incidents, learning)

4.2.6 Overarching activities

To support the management of all five risk areas, the PGS and the DDSM specifically identifies some key supporting activities, which are required as part of the DSP:

- Training and awareness
- Inspections and exercises
- Quality assurance
- Performance measurement

Training and awareness: Security training and awareness is one of the most effective risk mitigation strategies; it is specifically addressed in the DDSM which requires that each department has in place a security awareness program covering all aspects of departmental and government security to ensure that individuals are informed and regularly reminded of security issues and concerns and of their security responsibilities. Furthermore, the DDSM requires that the DSO, security practitioners and other individuals with specific security responsibilities should receive appropriate and up-to-date training to ensure they have the necessary knowledge and competencies to effectively perform their security responsibilities and do not inadvertently compromise security

The current lack of capacity to ensure ongoing security training and awareness across the Department, including the Regional Offices and SCCs, leads to a high likelihood that employees do not have a sufficiently high level of awareness of security threats and vulnerabilities.

Current training and awareness activities of the Department are currently being documented. Based on this work, a comprehensive program covering all aspects of security will be developed to ensure that individuals are properly trained and that their training is updated regularly. This program will include both training and awareness activities for departmental employees, as well as the training that is required for security personnel across the Department.

The objective is that all employees understand and comply with their security responsibilities, and that they do not inadvertently compromise security. Currently, some security awareness and training activities are delivered (e.g., 86% of employees have completed mandatory IT security training), but these activities are not yet comprehensive and there are no plans for regular refreshers.

Inspections and exercises: The DDSM provides information on inspections and exercises, which should be implemented to effectively manage any security program. Specifically, routine security inspections need to be conducted on sites or systems where sensitive information and assets are processed or stored to ensure compliance with security requirements (e.g., security inspections during limited-access hours).

In the context of emergency management, Business Continuity Plans are to be tested and readiness exercises conducted to ensure efficient and effective response and recovery in the context of a real emergency situation.

The work currently performed in this area for both security and emergency management will be documented and further elaborated to ensure compliance with all related requirements.

Quality assurance: Under the DDSM, a quality assurance plan must be developed and implemented to monitor security controls in place and oversee the ongoing effectiveness of controls. There is no comprehensive quality assurance plan for the HRSDC Security Program. However, a plan will be developed to define a coherent and encompassing means to ensure all controls are monitored and essential oversight is conducted for all security domains in all departmental facilities, including regional facilities and SCCs. Specifically, the Plan will seek to verify that identified security controls efficiently and effectively meet departmental security requirements.

Performance measurement: The ongoing measurement of the Department's performance in the delivery of the Security Program is a key component of the DSP to ensure that an acceptable level of risk is achieved and maintained.

Some security work is currently being measured, but more is required to create a comprehensive framework that will be used to report on the extent to which security activities and controls are achieving intended results. This work will be undertaken over the next few years. More specifically, performance indicators will be developed on the basis of the security controls that need to be in place. For more information, please see Section 5.2.

4.2.7 Controls to manage Security Risk Areas

This section presents information on the security controls currently in place for each of the key risks. It also identifies gaps, as well as the additional controls that were determined to be required in order to achieve security objectives and an acceptable level of residual risk.

1. Overarching activities

Controls in Place	Gap Analysis	Proposed Mitigating Strategies: Additional Controls
Availability of Resources	**Need to assess resource needs for security management**	Resource determination model (RDM) is being developed for IISD
Security training	**Comprehensive security training is not done consistently**	Develop a comprehensive security training and awareness program for all employees on all security requirements
IT security training	**None**	N/A
Security practitioners training	**Security training for security practitioners is not up-to-date**	Establish an inventory of security practitioners and positions, training required, taken and still needed. ITSCOE training inventory exists and a 3-yr training plan was developed (began in 2010-11)
Security awareness	**Security awareness activities are not done consistently**	Develop a comprehensive security training and awareness plan for all departmental security requirements
	Security intranet site content outdated	Security Intranet site to be updated. ITSCOE has a dedicated and up-to-date website
Quality assurance	**No comprehensive quality assurance plan as per PGS**	Develop a quality assurance plan
It security systems	**Some functions are transitioning to Shared Services Canada (SSC)**	Roles of SSC and IITB/HRSD to be clarified

Security inspections & exercises	**Inspections, exercises, tests not done systematically and consistently**	Develop a comprehensive inspection plan to ensure compliance with departmental security requirements
Security related internal documents	**Departmental security manual needs to be updated** **Ensure IM policy updates reflect security policy updates**	Departmental Security Manual currently being updated to reflect new security requirements

2. Security Risk Area 1: Information Assurance

Controls in Place	**Gap Analysis**	**Proposed Mitigating Strategies: Additional Controls**
Security provisions in arrangements and agreements	**Security procedures and directives on information disclosure to third parties are not always correctly applied by employees** **Regular review of arrangements and agreements not always done**	To create process requiring security sign-off on information sharing agreements to ensure managers understand their responsibility for considering potential security requirements in contracting documents Introduce a procedure to trigger internal review of new and changed information sharing agreements (to include DSO or delegate sign-off on ISAs, including IT-related and regional)
Sensitive information is categorized	**No automation of record-keeping, as required by TBS's Directive on Recordkeeping**	Develop and maintain a comprehensive, Department-wide inventory of protected and classified information; information should be linked to information owners to provide accountability for the maintenance of security classification
Quality assurance	**No quality assurance plan as mandated by the PGS**	Quality assurance plan to be developed

3. *Security Risk Area 2: Individual Security Screening*

Controls in Place	Gap Analysis	Proposed Mitigating Strategies: Additional Controls
Security level included job position descriptions	**No regular review of job descriptions to ascertain accuracy of security requirements**	Establish a procedure to review a sample of work descriptions on a regular basis - To include in the quality assurance plan
Security screening of employees	**Form TBS 330-47 is not consistently administered across the Department - no quality control of security screening files** **Inconsistency across departments, and the transfer of security files does not give full assurance of files' integrity**	Regularly review a sample of security screening files – To include in the quality assurance plan The revised TBS Standard on Individual Security Screening is expected to address certain issues, notably consistency in screening standards across departments
Security status field in CMS	**Identity and Access Management Framework not yet in place - Personnel position changes are not monitored for changes in access requirements**	Implement the Identity and Access Management Framework, which began in 2009, to increase the integrity of identity and access management controls, processes, procedures and data
Security Screening Certification for contractors	**PWGSC administration of TBS 330-47 may be inadequately tailored for HRSDC**	The revised TBS Standard on Individual Security Screening is expected to address this issue
Contractors' statements of work	**Outside of IITB, no regular review of statements of work or contracts are conducted to ascertain security requirements** **Managers responsible for contractors hiring do not always properly assess sensitivity of the information to be handled**	Establish regular and comprehensive review of a sample of statements of work or contracts – To include in the quality assurance plan. ITSCOE reviews IT-related statements of work ITSCOE is developing a process for IITB contractors, including tailoring the Security Requirements Checklist (SRCL) to be HRSDC-specific

4. *Security Risk Area 3: Physical Security and Access Control*

Controls in Place	Gap Analysis	Proposed Mitigating Strategies: Additional Controls
Physical access controls	**New access control system for NCR is required**	Planning underway for a NCR system with regional implementation, if appropriate - funding for new system is required

Physical security restrictions and controls **Protection of front-line staff**	Compliance with TBS standards for security zoning may conflict with service design of SCCs (i.e. no barriers between SCC officers and clients) Staff may not be sufficiently informed to recognize threats and react properly	Allocation of new resources is required – to be considered in RDM Security information specific to front-line staff to include in the security training, and awareness program to be developed
Threat and risk assessments (TRAs)	Comprehensive Security TRAs are not systematically conducted or updated TRAs recommendations not consistently implemented	Allocation of new resources is required – to be considered in RDM Establish mechanisms for continuous review of TRAs – to include in the quality assurance plan
	For information protection TRAs, templates need to be updated	Update templates as required – work currently underway IT Security templates are up-to-date
Secure filing cabinets	Some inventories are not being kept up-to-date	Conduct security reviews – to include in the inspection plan
Locks and cabinets	Cabinets and locks may not comply with applicable requirements in all facilities	Conduct security reviews – to include in the inspection plan
Security clauses for Private-sector companies	Some contracts are not reviewed. Some security clauses need to be updated	Allocation of new resources is required – to be considered in RDM Put in place a process requiring sign-off on all departmental contracts with security requirements
Personnel termination	Identity and Access Management Framework not yet in place	Implement the Identity and Access Management Framework, which began in 2009, to increase the integrity of identity and access management controls, processes, procedures and data.

5. *Security Risk Area 4: IT Security*

Controls in Place	Gap Analysis	Proposed Mitigating Strategies: Additional Controls
Overall ITSCOE Program Controls		Certification & Accreditation (C&A) Roadmap Project pending approval to C&A ~400 applications/systems and IT Infrastructure IITB C&A Approved Project is in place IT Security Policy Framework and Architecture to be finalized IT Security Change and Configuration to be put in place (Audit BCP 18)
IT Security awareness	IT security awareness not fully coordinated with IISD - discrepancies may arise.	Integration of all security domains in awareness sessions, and mandatory – to include in the security training and awareness

		program to be developed.
IT Security Policy	**Need alignment with Security Manual as it is updated**	DITS PoI will be updated to align with Departmental Security Manual and other TBS policy instruments. IT Security Policy Framework & Architecture to be finalized to complement DITS PoI.
Certification and Accreditation (C&A)	**Responsibility for HRSDC C&A is under ITSCOE/ IITB**	IITB is developing a strategic plan: Project #1 – to certify and accredit all FY approved IITB project; and Project #2 – to certify and accredit all ~400 applications/systems and IT Infrastructure
C&A scheduling and automation		ITSCOE has a process to manage all HRSDC C&A but as SSC is responsible for email, data centres and networks - ITSCOE will consult SSC as required.
IT infrastructure & applications TRAs	**IT solution/application and infrastructure TRAs to continue.**	Conduct a comprehensive assessment of the overall departmental Intranet infrastructure, including updating IT Infrastructure TRA.
Electronic data sharing agreements	**Shared responsibility with SSC has not yet been clarified.**	Roles of SSC and IITB/HRSD to be clarified - SSC is responsible for email, data centres and networks. ITSCOE will develop/update the ITS Policy in this regard.
Security Information and Event Management (SIEM)	**Shared responsibility with SSC has not yet been clarified.**	Roles of SSC and IITB/HRSD to be clarified for event management, audit, review and testing - SSC responsible for system audit, email, data centres and networks. ITSCOE will develop/update the ITS Policy in this regard. Coordination with the development of the IISD Incident Case Management System is necessary.
Network monitoring	**Transition to SSC**	Roles of SSC and IITB/HRSD to be clarified Perform independent validation and verification of the perimeter safeguards and security controls Qualitative analysis of data outflows and Data Loss Prevention technology to prevent transfer of sensitive data outside the departmental secure perimeter Continual review and renewal of IT security systems and products
IT infrastructure protection	**ITSCOE is responsible for solutions and applications/systems protection**	Roles of SSC and IITB/HRSD to be clarified Continue to integrate security activities as part of the System Development Life Cycle (SDLC) planning Establish security standards and best practices for development and testing of new applications

IT Hardware	**None except clarification of roles of SSC and IITB needed**	Roles of SSC and IITB/HRSD to be clarified SSC will implement the disintegrator tool that was purchased in FY 10/11 so that electronic media (e.g. Hard drives) can be securely destroyed.
Identity management:	**Identity and Access Management Framework not yet in place.** **User account monitoring needs strengthening and broader coverage**	Implement the Identity and Access Management framework, which began in 2009, to increase the integrity of identity and access management controls, processes, procedures and data
ITS Policy	**Ensure IT/ IM policy updates reflect security policy updates**	ITSCOE to develop IT/IM Security Policy Framework and Architecture.

6. *Security Risk Area 5: Incident Management, Emergency Management and Business Continuity*

Controls in Place	**Gap Analysis**	**Proposed Mitigating Strategies: Additional Controls**
Security incidents	**No Incident Case Management System in place for detailed, timely and informed analysis.**	Allocate adequate resources and funding for Incident Case Management System (ICMS) which will include all Regional and IT-related incidents Implement a standard approach to incident data gathering and analysis
	IISD Regions do not always report their security incidents to NHQ **IITB does not report IT related incidents to DSO**	Incident Case Management System (ICMS) will facilitate regional reporting ITSCOE will develop procedures on incident reporting in HRSDC, with DSO and ITSS Post-mortem and action log report will also be included
Security Incident Management Protocol	**Protocol needs to be updated**	Update the protocol when the ICMS Is further developed
Investigation of Security incidents	**None**	N/A
Strategic Emergency Management Plan (SEMP)	**SEM P is in place but additional resources required for implementation**	To be considered in RDM Specifically, a departmental emergency management exercise program will be developed and implemented
Departmental Business Continuity Management Program	**450 Business Continuity Plans for business lines and Service Canada Centres but BCPs are not regularly tested**	Continue development of department-wide, facility, and Regional BCPs Develop a plan for regular maintenance and testing – to include in the inspection plan

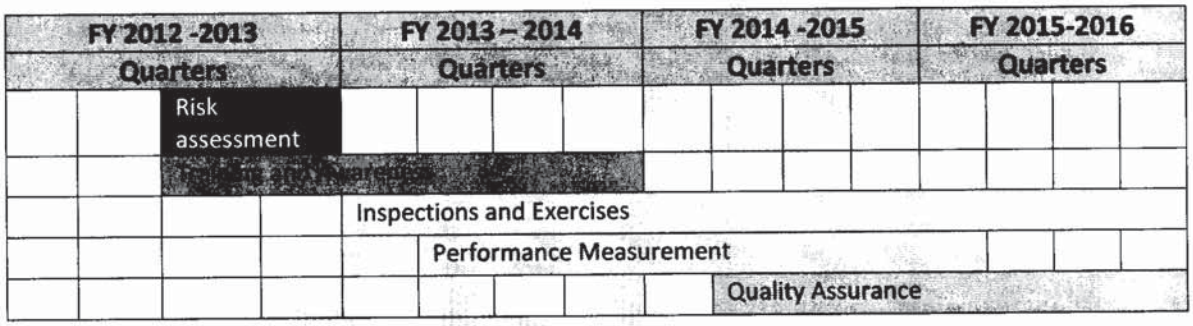
Other plans	Plans in place will require updating: - Pandemic Plan - Postal Disruption Plan - ESF 7 - Departmental readiness to respond to cyber incidents initiative	Develop schedules for regular review and update for Department
Business Impact Analysis	BIAs need regular review and updating	Develop schedule for regular BIA review and update, for department
HRSDC Critical Services (CS) list	2006 critical list needs to be updated	Update critical services list, based on department-wide BIA Update ITSCOE system list to ensure congruity between Critical Services and systems list
Fire protection and building emergency evacuation	Staff training in procedures is not mandatory, but is required by Canada Labour Code	Introduce mandatory training on procedures for fire, building and other emergencies – to include in the security training and awareness program
National Emergency Operations Centre (NEOC), Regional Emergency Operations Centres	Need review of staffing arrangements in event of need for 24/7 operations	More resources required – to be considered in RDM

5 Implementation, Measurement, Reporting and Update

5.1 Implementation Plan

A department-wide security risk assessment was undertaken several months ago, in line with existing requirements. As indicated above, this initiative will be refreshed and complemented over the next few months. This will be an opportunity to conduct a review of the current risks and the identification of any emerging risks. Furthermore, it will allow for the consideration of any additional measures that might be required to manage the Security Program effectively and to minimize residual risks.

With respect to the four overarching activities (see Section 4.2.6), the Department will focus on these activities and will document and further develop them to meet expectations. The following table indicates the sequence of development should resources be available. More details are provided in the Implementation Plan (Appendix A).



Also, IISD is in the process of developing a Resource Determination Model (RDM) to translate its operational workload requirements into resource terms in order to forecast resource requirements based on current and anticipated work. The RDM is forward looking, therefore modelled on what the HRSDC Security Program should look like rather than its current state. This initiative will seek to take into account the work required to fully implement the DSP over the next few years.

And in addition to these overarching elements, as resources become available, each lead will move forward with the more specific additional controls identified in the Implementation Plan (Appendix A).

5.2 Performance Measurement Strategy Framework

The ongoing measurement of the Department's performance in the delivery of the Security Program is a key component of the DSP to ensure that an acceptable level of risk is achieved and maintained. The TB *Guide on Developing a DSP* requires the development of

a Performance Measurement Strategy Framework (PM Strategy Framework), which identifies performance indicators to assess the effectiveness of controls included in the DSP. Expectations for such an initiative continue to evolve, as TBS is developing additional direction and guidance on security performance measurement.

Some security work is currently being measured, but more is required to develop a comprehensive framework that will include a range of performance indicators to assess and report on the extent to which security activities and controls are achieving intended results.

Using the *HRSDC Performance Measurement Guide,* which provides direction to ensure ongoing compliance and methodology for effective measurement, the HRSDC Security Program has started developing its PM Strategy Framework.

Specifically, HRSDC has developed a logic model to represent the activities of its Security Program and its intended results. This model will guide the development of performance measures over the next few years. It is based on 10 activities (see Appendix B):

1. Screen individuals
2. Provide training and awareness
3. Conduct inspections and exercises
4. Provide advice and direction
5. Develop threats and risks assessments
6. Develop plans, reports and tools
7. Manage IT security
8. Manage security controls
9. Manage incidents and emergencies
10. Conduct enquiries and investigations

Performance indicators and selected key performance Indicators will be developed on the basis of the logic model, and will align with the security controls that have been identified in the DSP.

5.3 Reporting

Monitoring implementation and reporting is key to the success of the Security Program: reporting reinforces the integration of security into business planning and priorities, and raises awareness of the role of security in meeting business objectives. The DSO will report progress on the implementation of the DSP, and eventually on the results of key performance indicators (KPIs), to the Deputy Minister and CMC, on a schedule to be established based on decisions pertaining to planning priorities.

5.4 Review and Update

The DSP will be reviewed at least annually. The DG-level Working Group on the DSP will continue to lead the work to be done to ensure a continual update of the plan, to adapt it to changing circumstances and to further guide the development of various elements and controls that are required to fully implement it.

Once a Performance Measurement Strategy Framework is in the place, the DSP will be updated based on the results of performance measurement, monitoring and oversight.

6 Building Capacity and Maturity

The HRSDC Security Program continues to evolve, in recognition of the importance of security as an enabler to achieve business objectives. Growth of the Program derives in part from resource transfers, in part from new funding. Resource transfers have served to integrate all security domains within one point of accountability – the DSO.

To continue building a strong culture of security and a robust Security Program for the Department, additional resources will need to be made available. HRSDC Security Program does not yet have the capacity to fully comply with existing requirements, notably the demands imposed by the DSP. As the Security Program matures, it is increasingly evident that facets of security are not being met and, as noted in the previous sections, some areas of security could be improved. Certain controls will need to be implemented as a result of reaching higher levels of capability maturity. One example of the latter currently being addressed by IISD is the need for accurate and timely statistical data on all elements of security, including incidents of all types, detailed security screening data, etc.

Appendix C presents a draft high-level maturity model. This will be developed over time in consultation with TBS and in tandem with TBS' development of a government-wide security maturity model.

Appendix A: DSP Implementation Plan

A. OVERARCHING ACTIVITIES TO MANAGE SECURITY RISK AREAS

Controls in Place	Gap Analysis	Proposed Mitigating Strategies: Additional Controls	Leader(s)	Time-frame Q/FY
1 Security **governance** both horizontal (cross-functional DG committee chaired by DSO, InSINC, NIISC) and vertical (DSO at CMC) exists Meetings are held regularly	None	N/A	ISB IISD and Regions[1]	-
2 Reorganization and restructuring of security resulting in one point of **accountability** for all areas of security, including regional offices ITSCOE is responsible for IT Security on behalf of HRSDC	None	N/A	ISB IISD and Regions IITB	-
3 Senior management ensures **resources** are available to ensure the necessary and defined security program is in place	Need to assess resource needs for security management in the department	Resource determination model (RDM) is being developed to translate operational workload requirements into resources terms (salary and non-salary) to forecast resource proposals This initiative takes into account the work required to implement the DSP over the next few years	IISD and Regions CFOB	3/12-13
4 **Security training** sessions in security domains are held regularly	Comprehensive security training in all security domains is not done consistently There is no requirement for training refresh on a regularly basis	Develop a comprehensive security training and awareness program for all employees on all security requirements (strategy to determine the validity period of each training) Allocation of new resources is required - to be considered in the RDM	IISD and Regions Service Canada College	3/12-13
5 **IT security training** is mandatory and is available via e-learning	None	N/A	ITSCOE	-
6 **Security practitioners** receive security **training**	Security training for all security practitioners is not up-to-date	Establish a department-wide inventory of security practitioners and security positions, training required, taken and still needed ITSCOE training inventory exists and	IISD and Regions ITSCOE	3/12-13

[1] In this table, "Regions" refers to the four Regional Executive Directors of Integrity and Regional Security Managers. The four REDs would be responsible for this in the four Regions.

Controls in Place	Gap Analysis	Proposed Mitigating Strategies: Additional Controls	Leader(s)	Time-frame Q/FY
		assessments of IT security professionals are needed Training streams have been identified and a 3-yr training plan developed (which began in 2010-11)		
7 Security **awareness** information is made available	Security awareness activities are not done consistently	Develop a comprehensive security training and awareness plan for all departmental security requirements	IISD and Regions ITSCOE	3/12-13
	Security intranet site content outdated	Security Intranet site to be updated ITSCOE has a dedicated and up-to-date website populated with IT security awareness information and self-study materials	IISD and Regions ITSCOE	3/12-13
8 Some **quality assurance** and data integrity processes are in place	There is no comprehensive quality assurance plan as mandated by the Policy on Government Security (PGS)	Develop a quality assurance plan Allocation of new resources is required - to be considered in the RDM	IISD and Regions ITSCOE	2/14-15
9 **It security systems** in place	Some functions are transitioning to Shared Services Canada (SSC)	Roles of SSC and IITB/HRSD to be clarified	ITSCOE (IITB) ITSS (SSC)	-
10 Security **inspections & exercises** are conducted regularly	Inspections, exercises, tests not done systematically and consistently across the Department	Develop a comprehensive inspection plan to ensure compliance with departmental security requirements Also, a departmental emergency management exercise program will be developed and implemented for the testing of the Strategic Emergency Management Plan (SEMP) Allocation of new resources is required – to be considered as part of the RDM	IISD and regions ITSCOE	2/13-14
11 Security related **internal plans, policies, guidelines and tools** are in place	Departmental security manual needs updating Ensure IM policy updates reflect security policy updates	Departmental security manual currently being updated to reflect new security requirements	IISD and regions ITSCOE	12-13

B. SECURITY RISK AREA 1: INFORMATION ASSURANCE

Controls in Place	Gap Analysis	Proposed Mitigating Strategies: Additional Controls	Leader(s)	Time-frame Q/FY
12 Arrangements and agreements (eg Vital events agreements, service level agreements, and/or arrangements with provincial and territorial governments,	Security procedures and directives on information disclosure to third parties are not always known, correctly understood or are not interpreted correctly by employees	Put in place a process requiring security sign-off on information sharing agreements to ensure managers understand their responsibility for considering potential security requirements in contracting documents	IISD and Regions ATIP	12-13

Controls in Place	Gap Analysis	Proposed Mitigating Strategies: Additional Controls	Leader(s)	Time-frame Q/FY
organizations or countries) incorporate relevant privacy and security responsibilities	Regular review of arrangements and agreements not always done	Introduce a procedure to trigger internal review of new and changed information sharing agreements (to include DSO or delegate sign-off on ISAs, including IT-related and Regional)	ISB	TBD
13 **Information is identified and categorized in terms of its sensitivity** as Protected in the non-national interest or classified as Confidential, Secret or Top Secret in the national interest	Automation of record-keeping, which is essential to ensuring compliance with the Treasury Board Secretariat's Directive on Recordkeeping	Develop and maintain a comprehensive, Department-wide inventory of protected and classified information; information should be linked to information owners to provide accountability for the maintenance of security classification	IITB	TBD
14 **Quality assurance** and data integrity processes are in place, but not documented: - Segregation of duties - Cross-referencing client information with provincial records - System audit logs	There is no comprehensive quality assurance plan as mandated by the PGS	To include in the quality assurance plan	IISD and Regions ITSCOE (IITB) SSC	2/14-15

C. SECURITY RISK AREA 2: INDIVIDUAL SECURITY SCREENING

Controls in Place	Gap Analysis	Proposed Mitigating Strategies: Additional Controls	Leader(s)	Time-frame Q/FY
15 **Job descriptions** contain types of information and commensurate with levels of sensitivity that the incumbent is authorized to access	No regular review of position descriptions to ascertain accuracy and presence of security requirements commensurate with levels of sensitivity to be accessed	Establish a procedure for regularly scheduled review of a sample of position descriptions - To include in quality assurance plan	IISD and Regions HRB	2/14-15

16 All HRSDC **employees are security screened** in accordance with TBS policy and standards	Form TBS 330-47 is not consistently administered across the department - there is no review of security screening files to ensure all steps are conducted appropriately	Regularly review a sample of security screening files to ensure compliance with policy and standards, to ensure consistency of background checks in security screening with changes of personnel to different positions – include in the quality assurance plan to be developed	IISD and Regions	2/14-15
		As required, the Security Program will supplement the TB 330-47 with a department-specific briefing focusing on the specific threats to HRSDC for both employees, as ITSCOE now does for IITB employees and contractors Employees will be briefed when they change positions, resulting in a change in security level	IISD and Regions	3/12-13
	Until updated direction is provided by Treasury Board (Operational Security Standard on Personnel Screening), there is inconsistency across departments, and the transfer of security files between departments does not give full assurance of the file's accuracy and integrity	The revised TBS *Standard on Individual Security Screening* is expected to address certain issues, notably consistency in screening standards across departments	IISD and Regions	-
17 A **security status field in the Corporate Management System** (CMS) displays employees' security screening status and validity period HR advisors are alerted that letters of offer may be issued only when the individual's screening status matches the security requirements identified in the job description	Identity and Access Management Framework not yet in place - Personnel position changes are not monitored for associated changes in access requirements Some Regions do not have systems in place to notify security of screening expiry date	Implement the Identity and Access Management framework, which began in 2009, to increase the integrity of identity and access management controls, processes, procedures and data	IISD and Regions HRB CFOB	TBD
18 TBS 330-47 **Security Screening Certification** and Briefing form is administered by PWGSC for **contractors**	PWGSC administration of TBS 330-47 may be inadequately tailored for HRSDC	The revised TBS *Standard on Individual Security Screening* is expected to address certain issues, notably consistency in screening standards across departments	-	-

19 **Contractors' statements of work** contain types of information and commensurate levels of sensitivity that contractors are authorized to access	Outside of IITB, there is no regular review of statements of work or contracts to ascertain accuracy and presence of security requirements commensurate with levels of sensitivity to be accessed	Establish a procedure for regularly scheduled review of a sample of statements of work or contracts, comprehensively – to include in the quality assurance plan	IISD and Regions CFOB	2/14-15
	Managers responsible for contractors hiring may not always properly assess the sensitivity of the information to be handled by the contractors	ITSCOE is developing a process for IITB contractors, including tailoring the Security Requirements Checklist (SRCL) to be HRSDC-specific ITSCOE does review IT-related statements of work	ITSCOE	12/14

D. SECURITY RISK AREA 3: PHYSICAL SECURITY AND ACCESS CONTROL

Controls in Place	Gap Analysis	Proposed Mitigating Strategies: Additional Controls	Leader(s)	Time-frame Q/FY
20 **Physical access controls** are in place in most facilities	New access control system for NCR is required	Planning underway for a standard access control system throughout the NCR and future Regional implementation where standardized approach is appropriate funding for new system is required	IISD and Regions CFOB	12-13
21 Key **physical security restrictions** and controls are in place Measures to **protect front-line staff** are in place in some Service Canada Centres (SCCs)	Strict compliance with TBS standards for security zoning and associated physical and electronic controls may conflict with the service design of SCCs (ie no barriers between SCC officers and clients)	Conduct and maintain update TRAs to determine where security zoning needs to be established or strengthened in some facilities Allocation of new resources is required – to be considered in the RDM	IISD and Regions	TBD
Front-line staff have procedures to deal with clients	Staff may not be sufficiently informed to recognize threats and react properly	Include in security training sessions, security information specific to front-line staff – to include in the security training and awareness program	IISD and Regions	3/12-13
22 **Threat and risk assessments (TRAs)** are conducted to determine physical security risks and provide mitigation strategies when an office modification or location change occurs or on a five-year cycle	Comprehensive, consistent department-wide, Branch and Region Security TRAs that address all areas of security are not systematically conducted or kept up to date	Allocation of new resources is required – to be considered in the RDM	IISD and Regions	TBD
	TRAs recommendations	Establish mechanisms for continuous review of	IISD and	2/14-15

Controls in Place	Gap Analysis	Proposed Mitigating Strategies: Additional Controls	Leader(s)	Time-frame Q/FY
	not consistently implemented	TRAs – to include in the quality assurance plan IT Security TRAs recommendations are implemented	Regions ITSCOE	- -
	For information protection TRAs, templates need updating	Update templates as required – work currently underway IT Security templates are up-to-date	IISD and Regions ITSCOE	12/13
23 **Inventories of secure filing cabinets** and access rights is regularly updated to prevent unauthorized disclosure of sensitive information	Some inventories are not be kept up-to-date	Establish a mandatory regular schedule for review of security equipment and staff access – to include in the inspection plan to be developed	IISD and Regions	2/13-14
24 **Locks and cabinets** used to store sensitive information comply with RCMP technical standards	Cabinets and locks may not comply in all facilities	Conduct security reviews – to include in the inspection plan	IISD and Regions	2/13-14
25 HRSDC contracts contain required **security clauses for Private-sector companies** that contract with the Department for the provision of services or products must comply with GC security requirements when handling government information and assets	Some contracts are not reviewed and some security clauses require an update	Allocation of new resources is required – to be considered in the RDM Put in place a process requiring security sign-off on all departmental contracts with security requirements to ensure managers and contracting officers understand their responsibility for considering potential security requirements in contracting documents	IISD and Regions	TBD
26 HRSB informs IISD on **personnel termination** forms for the return of sensitive or other information and assets	Identity and Access Management Framework not yet in place - Personnel position changes are not monitored for associated changes in access requirements	Implement the Identity and Access Management framework, which began in 2009, to increase the integrity of identity and access management controls, processes, procedures and data	IISD and Regions HRB CFOB	TBD

E. SECURITY RISK AREA 4: IT SECURITY

Controls in Place	Gap Analysis	Proposed Mitigating Strategies: Additional Controls	Leader(s)	Time-frame Q/FY
27. **Overall ITSCOE Program Controls** in place Ongoing activities: IT BCP,		Certification & Accreditation (C&A) Roadmap Project pending approval to C&A ~400 applications/systems and IT Infrastructure IITB C&A Approved Project is in place	ITSCOE	- End of

Controls in Place	Gap Analysis	Proposed Mitigating Strategies: Additional Controls	Leader(s)	Time-frame Q/FY
IT Awareness, IT Security Architecture, IT Security Audit		IT Security Policy Framework and Architecture to be finalized IT Security Change and Configuration to be put in place (Audit BCP 18)		12/13 End of 12/13 End of 12/13
28. Mandatory **IT Security awareness** is given regularly and widely accessible on Intranet ITSCOE participates in Security Awareness Week	IT security awareness is not fully coordinated with IISD awareness. Discrepancies may arise, as IISD comprehensive security awareness is not mandatory	Integration of all security domains in awareness sessions, and mandatory – to include in the security training and awareness program to be developed	IISD and Regions ITSCOE	To begin 3/12-13
29. ITSCOE has developed and published the HRSDC **Policy** on Departmental IT Security Management which is regularly reviewed and updated	Alignment with Departmental Security Manual as it is updated	Review for consistency with updated security manual The DITS PoI will be updated to align with Departmental Security Policy and other TBS policy instruments IT Security Policy Framework and Architecture to be finalized to complement the DITS PoI	ITSCOE	12/14 End of 12/13
30. **Certification and Accreditation** (C&A) of most IT systems is conducted under the IT Security Accreditation Program	Responsibility for HRSDC C&A is under ITSCOE/ IITB. ITSCOE will consult SSC on a required basis	IITB is developing a strategic plan. Project #1 – to certify and accredit all FY approved IITB project. Project #2 – to certify and accredit all ~400 applications/systems and IT Infrastructure.	ITSCOE	 12-15 12-15
31. IITB has a process in place to facilitate **C&A**, including scheduling, automation of C&A process, training and tools for managers, and to ensure that capacity to do C&A for high-sensitivity systems exists in-house.		ITSCOE has a process to manage all HRSDC C&A but as SSC is responsible for email, data centres and networks, ITSCOE will consult SSC as required.	ITSCOE SSC	-
32. IT infrastructure and applications **TRAs** are conducted, as part of C&A. Ongoing review and assessment of Internet and Intranet security is conducted.	ITSCOE will continue conducting IT solution/application and infrastructure TRAs.	Conduct a comprehensive assessment of the overall departmental Intranet infrastructure that will include updating departmental IT Infrastructure TRA to assess its current security posture.	ITSCOE SSC	12-15
33. Security specifications	Depending on the specific	Roles of SSC and IITB/HRSD to be clarified	ITSCOE	13-14

Controls in Place	Gap Analysis	Proposed Mitigating Strategies: Additional Controls	Leader(s)	Time-frame Q/FY
in **electronic data sharing agreements** (other departments, other governments, third parties) are included and reviewed for accuracy and relevance ITSCOE is developing a data "Gateway" to address Service Level Agreements, MOUs, etc	Information Sharing Agreement (ISA), IITB will consult SSC	SSC is responsible for email, data centres and networks. ITSCOE to establish partnership with SSC. ITSCOE will develop/update the ITS Policy in this regard	SSC	
34. IITB is currently implementing a **Security Information and Event Management** (SIEM) system, which permits a centralization and analysis of a comprehensive collection of all systems events ITSCOE conducts system audit, reviews and tests	Shared responsibility with SSC has not yet been clarified for event management, audit, review and testing - SSC responsible for system audit.	Roles of SSC and IITB/HRSD to be clarified SSC is responsible for email, data centres and networks. ITSCOE to establish partnership with SSC ITSCOE will develop/update the ITS Policy in this regard Coordination with the development of the IISD Incident Case Management System is necessary.	ITSCOE SSC	13-14
35. Continuous **network monitoring** to counter threats, vulnerabilities and unauthorized access: - Network perimeter monitoring and intrusion prevention devices/systems - Review of industry vulnerability advisories	Transition to SSC.	Roles of SSC and IITB/HRSD to be clarified Perform independent validation and verification of the perimeter safeguards and security controls, with increasing strength commensurate with increasing assurance level Qualitative analysis of data outflows and Data Loss Prevention technology to prevent transfer of sensitive data outside the departmental secure perimeter Continual review and renewal of IT security systems and products	SSC	-
36. **IT infrastructure protection** controls are in place. IT solution protection controls are in place	ITSCOE is responsible for solutions and applications/systems protection	Roles of SSC and IITB/HRSD to be clarified Continue to integrate security activities as part of the System Development Life Cycle (SDLC) planning Establish security standards and best practices for development and testing of new applications	ITSCOE SSC	12-15
37. **Hardware** lifecycle is now managed by SSC, based on processes established by IITB	None except clarification of roles of SSC and IITB needed	Roles of SSC and IITB/HRSD to be clarified SSC will implement the disintegrator tool that was purchased in FY 10/11 so that electronic media (e.g. Hard drives) can be securely destroyed	ITSCOE SSC	-

Controls in Place	Gap Analysis	Proposed Mitigating Strategies: Additional Controls	Leader(s)	Time-frame Q/FY
38. **Identity management**: Information from HRSB enables monitoring and changing user access based on position changes and terminations, to ensure changes in access requirements	Identity and Access Management Framework not yet in place User account monitoring needs strengthening and broader coverage	Implement the Identity and Access Management framework, which began in 2009, to increase the integrity of identity and access management controls, processes, procedures and data - Automated provisioning and de-provisioning of system access - System access reports that enable managers to audit and respond to appropriate employee access and use. - Additional user controls are needed; e.g., strengthened encryption	HRB ITSCOE SSC	13-14
39. **ITS Policy** is published on the Intranet. Information management policies reflect information security	Ensure IT/ IM policy updates reflect security policy updates	ITSCOE to develop IT/IM Security Policy Framework and Architecture	IISD ITSCOE	13-14

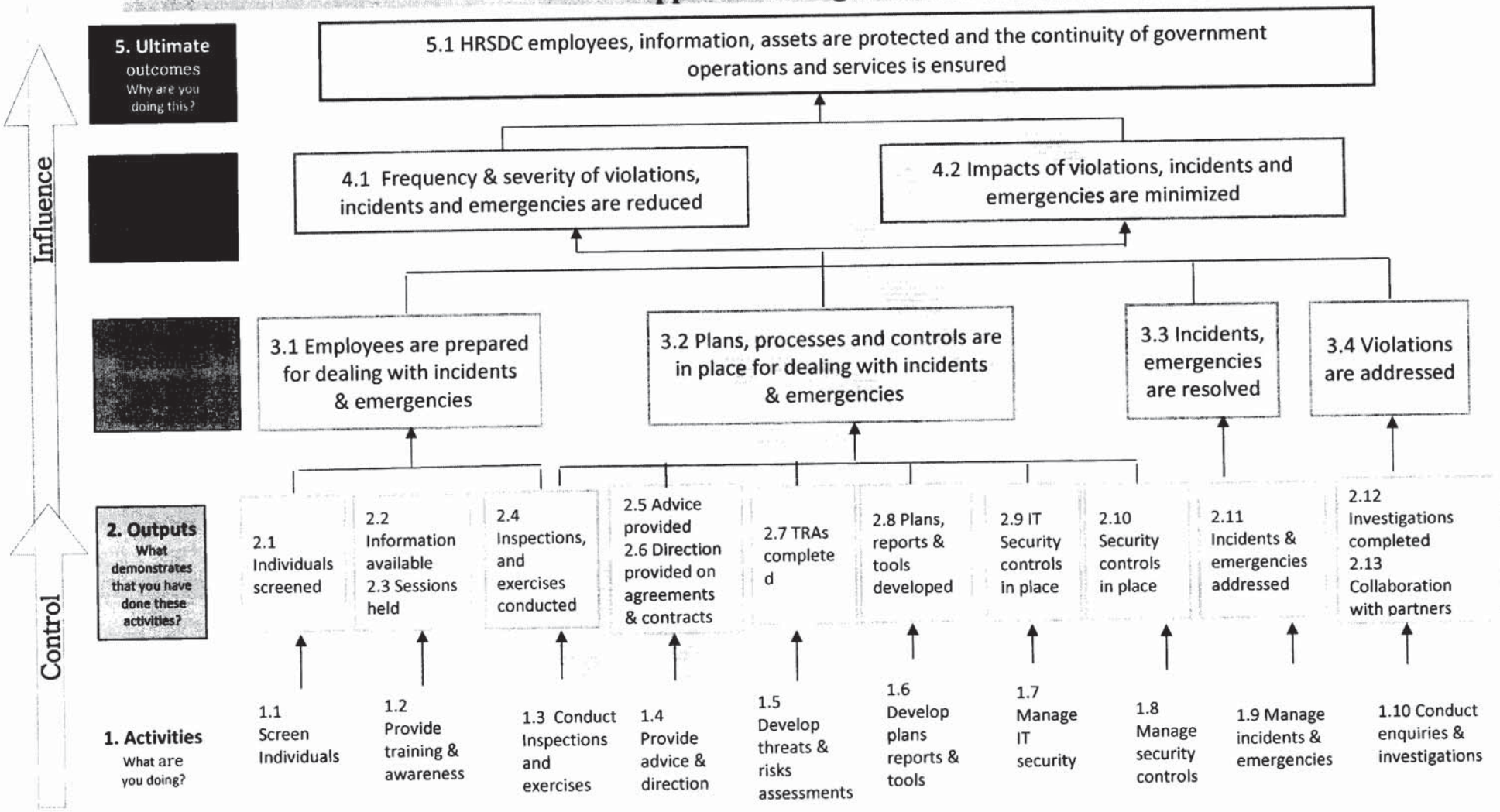
F. SECURITY RISK AREA 5: INCIDENT MANAGEMENT, EMERGENCY MANAGEMENT AND BUSINESS CONTINUITY

Controls in Place	Gap Analysis	Proposed Mitigating Strategies: Additional Controls	Leader(s)	Time-frame Q/FY
40. **Security incidents are managed**, and corrective actions are taken (on a case-by-case basis). NHQ Incident Management Unit is dedicated to security and privacy incident management; a process to report, resolve and assess security incidents has been established Through the DSO, IITB manages IT security incidents	IISD Regions do not always report their security incidents to NHQ IITB does not report IT related incidents to the DSO	An Incident Case Management System (ICMS) will facilitate regional reporting (see item below) ITSCOE will develop procedures on incident reporting in HRSDC, with DSO and ITSS. Post-mortem and action log report will also be included	IISD and Regions ITSCOE	TBD 12-13
	No Incident Case Management System in place for detailed, timely and informed analysis There is no means of quickly collating data or	Allocate adequate resources and funding for Incident Case Management System (ICMS) which will include all Regional and IT-related incidents Implement a standard approach to incident data gathering and analysis	IISD and Regions	TBD

Controls in Place	Gap Analysis	Proposed Mitigating Strategies: Additional Controls	Leader(s)	Time-frame Q/FY
	conducting over-time analysis of incident trends			
41. **Security Incident Management Protocol** for reporting personal incident disclosures has been developed and is posted on the Security Intranet	Protocol needs to be updated	Update the protocol when the ICMS is further developed	IISD and Regions	TBD
42. Security incidents are **investigated** as necessary	None	N/A	IISD and Regions	-
43. Department-wide **Strategic Emergency Management Plan (SEMP)** is in place	SEMP is in place but additional resources required for implementation	A Resource determination model (RDM) is being developed to translate operational workload requirements into resources terms (salary and non-salary) in order to forecast resource proposals. The work required for the implementation of the SEMP will be considered in the development of the RDM. Specifically, a departmental emergency management exercise program will be developed and implemented	IISD and Regions	-
44. Departmental **Business Continuity Management Program** is in place for development and maintenance of BCPs across the portfolio	Program is in place. 450 Business Continuity Plans for business lines and Service Canada Centres but BCPs are not regularly tested	Continue development of department-wide, facility, and Regional BCPs Develop a plan for regular maintenance and testing – to include in the inspection plan	IISD and Regions	Ongoing 1/13-14
45. The following **plans are in place:** - Pandemic Plan - Postal Disruption Plan - ESF 7 - Departmental readiness to respond to cyber incidents initiative	Plans in place will require updating: - Pandemic Plan - Postal Disruption Plan - ESF 7 - Departmental readiness to respond to cyber incidents initiative	Develop schedules for regular review and update	IISD and Regions	TBD
46. **Business Impact Analysis** (BIA) have been conducted department-wide and to be completed in 2012	BIAs need regular review and updating	Develop schedule for regular BIA review and update	IISD and Regions	2/14-15
47. HRSDC has a **Critical Services** (CS) list ITSCOE has a Critical Systems list which is regularly updated	2006 critical list needs to be updated	Update critical services list, based on department-wide BIA Update ITSCOE system list to ensure congruity between Critical Services and systems list	IISD and Regions ITSCOE	12-13
48. TBS standards on **fire protection and building emergency evacuation**	Staff training in procedures is not mandatory, but is	Introduce mandatory training on procedures for fire, building and other emergencies – to include in the security training and awareness	IISD and Regions	3/12-13

Controls in Place	Gap Analysis	Proposed Mitigating Strategies: Additional Controls	Leader(s)	Time-frame Q/FY
are being followed	required by Canada Labour Code	program to be developed		
49. The **National Emergency Operations Centre** (NEOC) and corresponding **Regional Emergency Operations Centres** are operational	Review of staffing arrangements in event of need for 24/7 operations	More resources required – to be considered in the RDM	IISD and Regions	TBD

Appendix B: Logic Model



Appendix C: Maturity Model

This table illustrates a draft maturity model for security which will be further developed to ensure progress in the evolution of the HRSDC Security Program.

1 **Initiated**	Leadership commitment to security Training & awareness activities developed & delivered on an ad hoc basis Incidents are managed on an ad hoc basis
2 **Defined**	All security domains integrated into one point of accountability (Departmental Security Officer) Key policies, standards and plans are in place with responsibilities and authority assigned Training and awareness material and activities developed & delivered regularly to targeted audiences Internal mechanisms developed to respond to incidents All staff and contractors are security screened Physical access controls in place in most departmental sites Inspections and exercises are conducted on an ad hoc basis Annual planning is done and basic quantitative data is collected
3 **Managed**	All levels of the organization share responsibility including managers and staff, and accountability is defined and communicated All policies, standards and plans are implemented across the department All employee participation in security training is mandatory Internal mechanisms fully implemented to respond to incidents Inspections and exercises are conducted regularly HRSDC's GoC back-up responsibilities are fully developed Quality review of security activities are planned Long-term and annual planning in place Performance Measurement Strategy Framework developed
4 **Sustainable**	Proactive systems in place to manage all aspects of security, including threat detection, and impact mitigation HRSDC is fully engaged with its partners to ensure interoperability of GoC and other partners' systems Progress on all security activities is monitored and reported to senior management
5 **Optimized**	HRSDC surpasses several or all GoC baseline security requirements Policies, standards and plans are consistently applied/used across the organization Security is fully integrated into all corporate (e.g. corporate risk profile) and business processes of the department (e.g. security in contracting) Security activities effectiveness is fully assessed over time

000518

PRIVACY AND IT SECURITY COMMITTEE (PISC)
RECORD OF DECISION
May 14, 2012

ITEM	AGENDA ITEM LEAD(S)	DECISIONS AND NEXT STEPS	ACTION ITEM LEAD(S)
Opening Remarks	P. Edwards M. Zommo	The Co-chairs welcomed members to the meeting, and noted the following: • PISC will be submitting a quarterly report to the Corporate Management Committee (CMC) for the meeting of May 18, 2012, • There will be a special PISC planning meeting on June 13, 2012. The purpose of the meeting is to discuss ways the committee can respond to strategic questions, and improve its overall effectiveness (e.g. update the PISC forward agenda integrating the privacy renewal action plan). • There are plans for an upcoming joint meeting between the Legal Issues Management Committee (LIMC) and PISC to discuss issues common to both committees.	
1. Review and Approval of Records of Decision	P. Edwards M. Zommo	The Record of Decision for the April 16, 2012 meeting was approved as circulated.	
2. Timing of Privacy Impact Assessments (PIAs)	J. Holden D. Todd	P. Edwards noted that CMC members discussed the importance of completing privacy impact assessments (PIAs) and certification and accreditation (C&A) processes before programs finalize information sharing agreements (ISAs) at the CMC meeting of April 20, 2012. CMC members also requested that PISC study the timing of, and responsibility for, PIAs. Summary of Discussion: • The committee discussed the timing of PIAs, C&A, ISAs, and PISC submissions. • PIAs and ISAs are sometimes reviewed after systems, programs, or agreements have gone 'live': privacy risks are not always identified and assessed from the outset. o Challenges were identified, including: (i) the complexity of the PIA requirements (ii) that responsibility and accountability for PIAs are not always clear, and (iii) that the development and approval process is cumbersome and time consuming. • Six (6) of the the 20 PIAs initiated by ATIP in 2011-2012 were completed. Members discussed how the PIAs were prioritized. • It was noted that an assessment should be completed by the programs at the outset to determine whether a PIA would be necessary, and, a general template with clear guidance would be helpful. • It was suggested that an umbrella PIA be developed to accommodate several programs which would support a more efficient process. • The new approach for developing PIAs should encourage substance and risk assessment, and not be overburdened by the process to prepare the PIA "report" as the outcome. Next Steps: • The process for PIAs must be simplified and streamlined to allow better efficiency. D. Todd will consult key stakeholders to develop a proposal, and will return to PISC with a proposed action plan. • J. Holden will review the remaining PIAs from 2011-2012 to triage, and consider cross-cutting risks while considering the groups with accountability on the file, and report back to PISC on the findings.	*D. Todd* *J. Holden*

ITEM	AGENDA ITEM LEAD(S)	DECISIONS AND NEXT STEPS	ACTION ITEM LEAD(S)
3. Medium Term Incremental (MTI) Performance Indicators for the Second Cycle of LMDA Evaluations	S. Johnson	The members considered proposed amendments to expand a longitudinal database that was created in 2008 to use it for the second cycle of LMDA evaluations. Highlights of the submission include: • Expansion of the current sample of 10% data held in the database to 100% for LMDA participants and to 20% for non-participants in the Territories and Atlantic provinces; • Use of the data held for the *MTI Performance Indicators Project* to undertake quantitative analyses for the second cycle of LMDA evaluations; and • Extension of the expiry date of the current MTI Performance Indicators Project from "March 31, 2013" to "March 31, 2017" and a similar extension to the data retention period. Summary of Discussion: • Members raised questions related to the volume of information requested, the nature of the projects being proposed and the request for data covering a 27 year period, which is beyond the previous practice of holding research data for 25 years. • S. Johnson noted that a PIA checklist had been completed and approved for the transfer of the data storage from the mainframe (PWGSC) to a mid-range server (Shared Services Canada) in the Data Development Directorate, SPRB and that a PIA checklist was in the final approval process for the proposed increase in the retention period for research data holdings from 25 years to 40 years, as requested by the Office of the Privacy Commissioner of Canada. Decision and Next Steps: • The Privacy and IT Security aspects of this project were approved subject to completion of the PIA process for the retention period and a C&A process if needed. • The committee agreed to recommend the project for Senior Associate DM signature, subject to these requirements.	*S. Johnson*
4. Passport Service Offering Evaluation	S. Johnson	As of January 2011, Service Canada established 144 Receiving Agent sites across Canada. According to the terms of the MOU between Passport Canada and HRSDC/Service Canada, it is Service Canada's responsibility to evaluate implementation issues and value of the Passport Service Offering. The evaluation will address performance (effectiveness, efficiency and economy), and will examine lessons learned against best practices of service delivery. Summary of Discussion: • R. Adcock asked for clarification on whether protected B level information would be collected using the online survey as it would require a higher level of security control. • From a privacy perspective this project is fairly straight-forward, however, an information sharing agreement will need to be in place before any exchange of personal information takes place for the evaluation. Decision and Next Steps: • The Privacy and IT Security aspects of this project were approved. • The Committee agreed to recommend the project for Senior Associate DM signature.	*S. Johnson*

000520

PRIVACY AND IT SECURITY COMMITTEE (PISC)
RECORD OF DECISION
May 14, 2012

ITEM	AGENDA ITEM LEAD(S)	DECISIONS AND NEXT STEPS	ACTION ITEM LEAD(S)
5. Preventive Mediation Impact Assessment Study	J. Garneau	No issues were raised by Committee members on the privacy and IT security aspects of the proposed study. Decision and Next Steps: • The Privacy and IT Security aspects of this project were approved. • The Committee agreed to recommend the project for Senior Associate DM signature.	*J. Garneau*
6. New Tort of Invasion of Privacy	S. Frost	Secretary's note: This item has been reviewed at LIMC and at CMC; it is presented to PISC for information purposes. The presentation provides an overview of recent developments, jurisprudence and status of the emerging tort of invasion of privacy in Canada. Next Steps: • Legal Services will provide updates in this area of the law as required.	*S. Frost*
7. Consolidation of Departmental Privacy Codes	S. Johnson S. Frost	The members received information on the Departmental Privacy Codes. A consolidation document was distributed that provides the changes that were made in the *Department of Human Resources and Skills Development Act.*	
8. HRSDC Approach to Open Government	C. Dea	The members were debriefed on the Department's effort on the open government initiative. Summary of Discussion: • The transformation will be large and will affect IT, Legal and Privacy. • The initiative will consider how to improve accessibility and transparency of the Department's data. • S. Johnson noted the need to engage other departments and the Office of the Privacy Commissioner of Canada as the approach is developed. • C. Dea noted that J. Holden and D. Todd have joined his working group. Next Steps: • C. Dea will provide further updates to PISC as required.	*C. Dea*
Next Meeting Date		*June 13, 2012, from 9:00 a.m. – 10:30 a.m.*	

PRIVACY AND IT SECURITY COMMITTEE (PISC)
RECORD OF DECISION
May 14, 2012

ATTENDANCE:

PRESENT	REGRETS	GUEST(S)	OBSERVERS
Rob Adcock Lorri Biesenthal Lucie Clément *for Daniel J. Comeau* Vincent DaLuz Peter Edwards (Co-chair) Susanne Frost Glennie Graham Jackie Holden Virginia Jakutavicius (*Ex Officio*) Stephen Johnson Julie Lalonde-Goldenberg Sylvain Patenaude Rakesh Patry *for Dominique La Salle* Mostafa Zommo (Co-chair)	Alexis Jonathan Conrad Marie-France Lamarche Donald Toussaint Mary Ann Triggs	Christian Dea Julie Garneau David Todd	Antonio Bakopoulos Geneviève Clavel Dawn Dirks Kathie Everett Joanne Leduc (Note taker) Thierry Rousseau

Corporate Management Committee (CMC) Forward Agenda

June	June	July	July	August
Wednesday **June 27, 2012** **1:30 p.m. - 3:30 p.m.**	**Friday** **June 29, 2012** **2:15 p.m. - 3:45 p.m.**	**Wednesday** **July 11, 2012** **1:30 p.m. - 3:30 p.m.**	**Wednesday** **July 25, 2012** **1:30 p.m. - 3:30 p.m.**	**Friday** **August 3, 2012** **9:30 a.m. - 11:30 a.m.**
• Departmental Security Plan (L. Beauséjour) • Cyber Threat Business Continuity Plans (L. Beauséjour) • Follow-up update on Playbook Pilot Project (P. Thompson / J. Lalonde) • Process Improvement Activities (A. Séguin) • Round table	• PASRB Budget Management (P. Larose) • HRSB Budget Management (P. Larose) • Corporate Commitments (P. Larose) • Semi-annual Contingent Liability Report (M. McCombs) • Round Table	• Disability Management: Proactive Management of Sick Leave (P. Larose) • Integrity Protocols (L. Beauséjour) • Sub-Committee Update: ADM Web (P. Larose) • Sub-Committee Update: LIMC (M. McCombs and P. Simeoni) • Round table	• IITB Budget Management – Including Understanding the Run (C. Nixon) • Corporate Secretariat Budget Management (S. Wiebe) • Round table	• Corporate Risk Profile: Mitigation Strategy Update (D. McGovern) • Legal Services Yearly Plan Overview (M. McCombs) • CFOB Moving Towards Efficiencies and Savings (A. Séguin) • Sub-Committee Update: IRC (P. Simeoni) • Round table

August	August	September	September	September
Wednesday **August 8, 2012** **1:30 p.m. - 3:30 p.m.**	**Wednesday** **August 22, 2012** **1:30 p.m. - 3:30 p.m.**	**Wednesday** **September 5, 2012** **1:30 p.m. - 3:30 p.m.**	**Friday** **September 7, 2012** **10:00 a.m. - 12:00 p.m.**	**Wednesday** **September 19, 2012** **1:30 p.m. - 3:30 p.m.**
• Integrated Risk Management Action Plan: Progress Report (D. McGovern) • National Accommodations Plan (A. Séguin) • Paid Union Leave – Review practice (P. Larose) • Round table	• Departmental Critical Services List (L. Beauséjour) • Information Management Strategy Update (C. Nixon) • Sub-Committee Update: PISC (S. Wiebe) • Sub-Committee Update: MPIB (A. Séguin and J. Paquette) • Round table	• Cyber Threat Table Top Exercise: Sr. Mgmt. Participation (L. Beauséjour – TBC) • Procurement within HRSDC - includes project-based procurement (A. Séguin) • Department Environmental Scan (D. McGovern) • Telework (P. Larose – TBC) • Round table	• Printer Policy (C. Nixon) • Information and Communication Technology Renewal (C. Nixon) • HRSDC's Duty to Accommodate Guidelines: Enhanced Section on Family Status (P. Larose) • Sub-Committee Update: ADM Web Committee (J. Gilbert) • Round Table	• Staffing Management Accountability Framework (SMAF) (P. Larose) • Internal Controls over Financial Reporting: Progress Update (A. Séguin – TBC) • Action Plan on Accounts Receivable – including MOU with CRA (A. Séguin) • Round table

Note: The CMC Forward Agenda was compiled using input from Branches. All items specified above will be added to the Corporate Secretariat's Integrated Forward Agenda (IFA).
Updated: June 21, 2012

Corporate Management Committee (CMC) Forward Agenda

October	October	October	November	November
Wednesday October 3, 2012 1:30 p.m. - 3:30 p.m.	**Wednesday October 17, 2012 1:30 p.m. - 3:30 p.m.**	**Wednesday October 31, 2012 1:30 p.m. - 3:30 p.m.**	**Wednesday November 14, 2012 1:30 p.m. - 3:30 p.m.**	**Wednesday November 28, 2012 1:30 p.m. - 3:30 p.m.**
• Operational Plan for Common Learning Offers (P. Larose and C. Giliberti – TBC) • Containing Cost and Risk: Hardware Rationalization (C. Nixon) • PCMAF Results (including DSAR) (P. Larose) • Sub-Committee Update: LIMC (P. Simeoni / M. McCombs) • Sub-Committee Update: IRC (P. Simeoni) • Round table	• Managed Print Services: Vendor Management (C. Nixon) • Desk Top Collaboration (C. Nixon) • HRSDC Management of Accounts Receivable (A. Séguin– TBC) • Containing Cost and Risk: PC Device Directive (C. Nixon) • Round table	• Annual Lessons Learned from Past Audits (V. DaLuz) • HRSDC Code of Conduct (L. Beauséjour – TBC) • Current FY Departmental Financial Statements (A. Séguin) • Round Table	• Intellectual Property (A. Séguin) • New Gatineau Tower (A. Séguin) • ATIP New Reporting Element (S. Wiebe) • Sub-Committee Update: PISC (S. Wiebe) • Sub-Committee Update: MPIB (A. Séguin and J. Paquette) • Round Table	• Windows 7 (C. Nixon) • Application Portfolio Management (C. Nixon) • Poor Performers Pilot (P. Larose) • Financial Policy Revitalization Plan Update (A. Séguin) • Round Table

Upcoming CMC Items					
	Finance	**Human Resources**	**IM/IT**	**Planning / Reporting**	**Other**
Target Date Unconfirmed		• Structural Model for Labour Relations (P. Larose) • Canada School of the Public Service: Language Training (P. Larose and C. Giliberti) • Workforce of the Future Strategy (P. Larose and C. Giliberti)			• General Approach to CRA (A. Séguin) • Directive to Departmental Employees: Responding to Security Incidents Involving Personal Information (L. Beauséjour)
Items with Target Date	• Departmental Investment Plan (A. Séguin - Dec. 2012) • Status report on current Major Projects and Investments (A. Séguin - Feb. 2013) • Internal Controls over Financial Reporting: Progress Update (A. Séguin - Mar. 2013) • CFOB Yearly Plan Overview (A. Séguin - Mar. 2013) • Current FY Departmental Financial Statements (A. Séguin - Sep. 2013)	• Integrated People Management: 3-year Strategy (P. Larose - Jan. 2013) • Review People Management Scorecard Indicators (P. Larose - Mar. 2013) • Report on 2012-13 People Management Priorities (P. Larose - late Mar. 2013) • Official Languages Training Framework (P. Larose and C. Giliberti - Mar. 2013) • HRSB Yearly Plan Overview (P. Larose - Mar. 2013) • EX PMP and TM (P. Larose - Mar. 2013)	• Alternate Service Delivery / Sourcing Options (C. Nixon - Jan. 2013) • Information Management Strategy Update (C. Nixon - Jan. 2013) • Update on Portfolio of IT Projects (C. Nixon - Feb. 2013) • IITB Yearly Plan Overview (C. Nixon - Mar. 2013)		• Sub-Committee Update: ADM Web Committee (J. Gilbert - Dec. 2012) • Departmental Sustainable Development Strategy: Update (A. Séguin - Dec. 2012) • Emergency Support Function (L. Beauséjour - March 2013) • ISB Yearly Plan Overview (L. Beauséjour - Mar. 2013) • Semi-annual Contingent Liability Report (M. McCombs – Dec. 2012 and Jun. 2013)

Note: The CMC Forward Agenda was compiled using input from Branches. All items specified above will be added to the Corporate Secretariat's Integrated Forward Agenda (IFA).
Updated: June 21, 2012