Agriculture and Agri-Food Canada | Agriculture et Agroalimentaire Canada
Canadian Food Inspection Agency | Agence canadienne d'inspection des aliments

REPORT:
Audit of Information Technology (IT) Security

AAFC Office of Audit and Evaluation

CFIA Audit and Evaluation Branch

Canada

The AAFC Audit Committee recommended this audit report for approval by the Deputy Minister on February 4, 2015.

The CFIA Audit Committee recommended this audit report for approval by the President on May 29, 2015.

Audit of Information Technology (IT) Security

Electronic version available at
AAFC www.agr.gc.ca/aud_eval
CFIA www.inspection.gc.ca/about-the-cfia/accountability/other-activities/audits-reviews-and-evaluations/eng/1299843498252

Catalogue No. A29-1/3-2015E-PDF
ISBN 978-0-660-01964-2
AAFC No. 12348E

Paru également en français sous le titre
Vérification de la sécurité de la technologie de l'information

For more information, reach us at
AAFC: www.agr.gc.ca or call us toll-free 1-855-773-0241
CFIA: www.inspection.gc.ca or call toll-free 1-800-442-2342

TABLE OF CONTENTS

Page

EXECUTIVE SUMMARY

Agriculture and Agri-Food Canada (AAFC) and the Canadian Food Inspection Agency (CFIA) manage sensitive digital information, and IT security has become a significant concern, given the increasing sophistication and prevalence of IT threats, as well as the public's increasing awareness and expectations related to the safeguarding of their information by organizations. AAFC and CFIA's operational environments pose challenges from an IT Security perspective, given their decentralized nature, with regional operations across the country. Furthermore, the IT and operational environments of AAFC and CFIA are undergoing renewal and transformation.

AAFC and CFIA have been impacted by the creation of Shared Services Canada (SSC) and the resulting consolidation of IT infrastructure-related services for the Federal Government of Canada. In the summer of 2011, IT infrastructure-related services that were formerly performed by AAFC and CFIA were transitioned to SSC. This consolidation included the monitoring of the security detection devices related to the IT infrastructure and the transition of AAFC and CFIA personnel who carried out these services.

Managing IT security has been and remains a top priority for AAFC, CFIA and SSC.

The audit included a review of the processes and controls in place at AAFC and CFIA to oversee and govern the IT Security related services provided by SSC.

The AAFC's Information Systems Branch (ISB) and CFIA's Information Management and Information Technology (IMIT) Branch report to the same individual who holds dual positions: AAFC's Assistant Deputy Minister (ADM) ISB and CFIA's Vice President, IMIT. AAFC is a third party service provider for CFIA for the provision of IT systems, including the corporate financial and human resources (HR) systems. Given the above, and the interconnectedness of AAFC and CFIA's operational environments, as well as similarities in relation to the potential IT security challenges, both organizations considered the benefits of conducting a joint IT Security Audit.

As federal government entities, both AAFC and CFIA are required to adhere to the Treasury Board's baseline security requirements as outlined in the Policy on Government Security (PGS) and related directives, standards and guidance.

The IT Security audit was included in AAFC's 2013-2016 Risk-Based Audit Plan and the CFIA's 2013-2016 Risk-Based Audit Plan. As IT security was identified as a significant risk, the objective of the audit was to provide assurance that AAFC and CFIA have adequate controls related to IT security in place for their IT systems, and these controls were operating efficiently and effectively. The scope of the audit focused on current IT security-related processes in place within AAFC and CFIA, with audit testing focused on the 2013-14 fiscal year.

As identified throughout the report, AAFC and CFIA have taken a number of positive steps related to IT security. Despite this, the audit found that gaps exist in the current IT security control framework. Opportunities for improvement in order to address these gaps are related to IT security governance, IT security risk management, security controls related to third party service providers, the management of sensitive digital information, physical security to IT assets, IT security risk assessment related to IT systems, and the implementation of logical access controls for IT systems. The audit provides a number of recommendations to address these identified gaps. While the audit focused on the management control framework for IT security, there were no specific security breaches identified.

1.0 INTRODUCTION

1.1 BACKGROUND

1.1.1 For any organization with sensitive digital information assets such as AAFC and CFIA, IT security has become a significant concern. This is due both to the increasing sophistication and prevalence of IT threats as well as the public's increasing awareness and expectations related to the safeguarding of their information by organizations. AAFC and CFIA's operational environments are challenging from an IT Security perspective, given their decentralized nature, with regional operations across the country. Furthermore, the IT and operational environments of AAFC and CFIA are undergoing renewal and transformation.

1.1.2 AAFC and CFIA have also been significantly impacted by the creation of Shared Services Canada (SSC). In the summer of 2011, IT infrastructure-related services that were formerly performed by AAFC and CFIA were transitioned to SSC, this included the monitoring of the security detection devices related to the IT infrastructure. This also included the transition of AAFC and CFIA personnel who carried out these services.

1.1.3 The AAFC's Information Systems Branch (ISB) and CFIA's Information Management and Information Technology (IMIT) Branch report to the same individual who holds dual positions: AAFC's ADM ISB and CFIA's Vice President, IMIT. AAFC is a third party service provider for CFIA for the provision of IT systems, including the corporate financial and human resources (HR) systems. Given the above, and the interconnectedness of AAFC and CFIA's operational environments, as well as similarities in relation to the potential IT security challenges, both organizations considered the benefits of conducting a joint IT Security Audit.

1.1.4 As federal government entities, both AAFC and CFIA are required to adhere to the Treasury Board's baseline security requirements as outlined in the Policy on Government Security (PGS) and related directives,

standards and guidance. IT security includes security related to any equipment or system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It also includes all matters concerned with the design, development, installation and implementation of information systems and applications to meet business requirements.

Background Specific to AAFC

1.1.5 AAFC has developed an IT Security Program Framework, including IT Security policies and user guidance. Roles and responsibilities of senior management over the governance of IT Security within AAFC are specified in the IT Security Policy and a Departmental Security Plan (DSP) has been developed. Accountability for Security within the Department rests with the Departmental Security Officer (DSO). The DSO is part of the Corporate Management Branch (CMB) and reports security breaches or illegal acts to the Deputy Minister through the Director General (DG) of Asset Management and Capital Planning and the Assistant Deputy Minister (ADM) of CMB. The DSO acts as the focal point for departmental security issues and all formal security communications with the various lead agencies. The Information Technology Security Coordinator (ITSC) is the Chief of the Information Technology Security Risk Management (ITSRM) team. The ITSC is part of ISB and has a functional reporting relationship to the DSO. The ITSC is responsible for advising and assisting the DSO and ADM ISB in managing the departmental IT security portion of the departmental security program.

Background Specific to CFIA

1.1.6 CFIA has implemented an IT Security Program Framework, including IT Security policies and an overall Agency Security Plan (ASP). Accountability for the ASP has been delegated to the Agency Security Officer (ASO). The ASO is the Director of the Assets and Security Management Directorate, Corporate Management Branch. The CFIA IT Security Directive indicates that the Agency Security Officer (ASO) is responsible for monitoring the implementation of security activities within the Agency and recommending appropriate remedial action to the Deputy Head or senior management committee (as appropriate) to address any deficiencies. The VP IMIT is responsible to ensure the effective and efficient management of the Agency's information and IT assets. The Agency’s ITSC is the Director of Information Technology Security Services & Architecture and is within the IMIT Branch that reports to the VP IMIT. The ITSC is responsible for the establishment and management of the CFIA IT security program, including developing an effective process to manage IT security incidents and promoting IT security in the Agency.

Although a direct reporting relationship between the ASO and the ITSC does not exist, there is a functional relationship through governance structures and an internal services agreement.

1.2 AUDIT OBJECTIVE

1.2.1 The IT Security audit was included in AAFC's 2013-2016 Risk-Based Audit Plan and the CFIA's 2013-2016 Risk-Based Audit Plan. The objective of the audit was to provide assurance that AAFC and CFIA have adequate controls related to IT security in place for their IT systems, and they were operating efficiently and effectively.

1.3 AUDIT SCOPE

1.3.1 The scope of the audit focused on current IT security-related processes in place within the organizations, with audit testing focused on the 2013-14 fiscal year.

1.3.2 The planning phase of the audit consisted of separate, broad IT security risk assessments for AAFC and CFIA. Separate risk workshops were conducted with representation from IT security, IT application development / support, Departmental / Agency Security Services, and program management for each organization. The workshops involved a further validation and input into the risk assessment.

1.3.3 Based on the risk assessment, lines of enquiry were developed for the audit related to:

- A governance structure for IT Security has been established for the Department / Agency and its relationship with partners and third parties.
- A formal process for the management of sensitive information assets exists and is consistently implemented to ensure the appropriate classification, use, and management of sensitive digital information.
- A formal process for IT security risk management is in place and implemented for IT systems.
- Logical access to systems is appropriately restricted to authorized users.

1.3.4 Audit activities were performed at AAFC and CFIA Headquarters in Ottawa as well as at selected regional locations. Audit activities were focused on those areas with higher concentrations of sensitive information as determined through the planning phase of the audit. The audit criteria used for the audit are provided in Annex A.

1.3.5 The scope of audit activity related to services that are the responsibility of SSC was limited to AAFC's and CFIA's processes and controls in place to oversee and govern those services provided by SSC.

1.4 AUDIT APPROACH

1.4.1 The approach and methodology used for the audit was consistent with the Internal Audit standards as outlined by the Institute of Internal Auditors (IIA), and aligned with the *Internal Audit Policy for the Government of Canada (GC).*

1.4.2 A risk-based audit program was developed that defined audit tasks to assess each audit criterion. Audit evidence was gathered through various methods including interviews, observations, analysis of data related to IT security practices, and document review. The conduct phase of the audit began in March 2014 and was completed by July 2014.

1.5 CONCLUSION

1.5.1 The AAFC Office of Audit and Evaluation (OAE) and the CFIA Audit and Evaluation Branch (AEB) concluded that gaps exist in the current IT security control framework. Opportunities for improvement in order to address these gaps that present the highest risk are related to IT security governance, IT security risk management, IT security risk assessment related to IT systems, the identification and safeguarding of Classified and Protected digital information, and the implementation of logical access controls for IT systems. Those gaps presenting a more moderate risk relate to the further formalization of security protocols related to travel, security controls related to third party service providers, and physical security to IT assets.

1.5.2 As the audit was focused on the management control framework for IT security and not identifying specific breaches, there were no specific security breaches identified.

These opportunities for improvement are presented in Section 2.0 of the report.

1.6 STATEMENT OF CONFORMATION

1.6.1 In the professional opinion of the Chief Audit Executives, sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the conclusion provided and contained in this report. The conclusion is based on a comparison of the conditions, as they existed at the time, against pre-established audit

criteria that were agreed on with management. The conclusion is applicable only to the entities examined.

1.6.2 This audit conforms with the *Internal Auditing Standards for the Government of Canada*, as supported by the results of the quality assurance and improvement program.

2.0 DETAILED OBSERVATIONS, RECOMMENDATIONS AND MANAGEMENT RESPONSES

2.0.1 This section presents the key observations, based on the evidence and analysis associated with the audit, and provides recommendations for improvement.

2.0.2 Management responses are included and provide:

- An action plan to address each recommendation;
- A lead responsible for implementation of the action plan; and,
- A target date for completion of the implementation of the action plan.

2.1 IT SECURITY GOVERNANCE

2.1.1 The audit expected that AAFC and CFIA have IT security frameworks that include a defined governance structure, including defined roles and responsibilities related to AAFC and CFIA's relationship with SSC.

2.1.2 From a governance perspective, roles and responsibilities between AAFC / CFIA and SSC related to IT Security are not always clear and at an operational level, have not been comprehensively defined. This is indicated through a number of examples, including:

- AAFC's Security Assessment & Authorization (SA&A) activities, including Threat and Risk Assessments (TRAs) and technical vulnerability assessments (VAs) identify application risks which are the responsibility of AAFC / CFIA versus infrastructure risks which fall under the responsibility of SSC. There is a no mechanism in place for AAFC / CFIA to inform or receive acknowledgement from SSC on the infrastructure risks identified.
- Although the transfer to ownership of larger data centres to SSC has taken place, AAFC and CFIA continue to be responsible for the actual granting of access to some of these locations, and in some cases SSC has requested AAFC and CFIA to update the access list. AAFC and CFIA staffs remain responsible for some of the smaller data centres in the regions. In some cases AAFC and CFIA staff were unsure of their

role in relation to these data centres, given SSC owns the IT infrastructure equipment in these data centres.

- SSC has administrative access to servers containing AAFC and CFIA data, including file shares on AAFC and CFIA network drives, and there is no formal mechanism between SSC and AAFC to discuss or track this access.
- Some activities, for example tape backups that are now the responsibility of SSC, are still being conducted in some regions by AAFC and CFIA staff. In one such situation, the backup tapes are kept for one year onsite and then moved across the street to a separate location, which is not a leading practice as this increases the risk of the loss of data if an incident such as a local disaster was to occur.
- Specific to AAFC, there is a transition plan in place for AAFC to take back responsibility for the antivirus software that is currently being administered by SSC. In the interim, although informed of incidents, AAFC has not received any reporting from SSC on trends or other analysis related to antivirus activities. Specific to CFIA, the employee that managed the antivirus system moved to SSC and CFIA is unaware of any activities that are currently being conducted related to this.
- Specific to AAFC, there is IT infrastructure equipment at research labs that was installed by the ISB staff at the lab that AAFC now considers to be under SSC responsibility, but this has not been communicated to SSC. This includes off the shelf wireless networking equipment purchased 15 years ago.

Findings Specific to AAFC

2.1.3 AAFC has a defined IT Security Governance Framework that involves the appropriate levels of management and representation from throughout the Department. The mandates and roles of IT security oversight bodies are consistent with leading practices and understood by key stakeholders within the Department; furthermore, these governance bodies meet on a regular basis. Key IT security governance committees include:

- Departmental Security Management Committee (DSMC);
- Security and Identity Steering Committee (SISC); and
- IT Security Working Group (ITSWG).

2.1.4 The Terms of Reference for the DSMC and SISC have not been updated since 2010, and, therefore does not consider the role of SSC. There is no formal Terms of Reference document for the ITSWG; although a description of the mandate and membership of the ITSWG is documented in the AAFC Departmental Security Plan (DSP) from February 2012. The ITSWG membership outlined in the DSP contemplates significant

representation from SSC. It was noted that during the audit period, a single SSC representative attended four of the seven ITSWG meetings, with no SSC representative in attendance at the other three meetings. SSC was only specifically mentioned in the minutes and records of decision in two of the seven ITSWG meetings.

Findings Specific to CFIA

2.1.5 CFIA has established the Security Program Management Committee (SPMC), a consultative and review committee that reports through the Agency governance structure, and is mandated to assist in the planning and implementation of the Agency Security Plan (ASP). Although the SPMC is intended to meet on a quarterly basis, given turnover at the Agency Security Officer level, the committee only met twice during the 2013-14 fiscal year. SSC was not specifically mentioned in the minutes for either of the two meetings. A more operational working group focused on IT security does not exist within the Agency.

2.1.6 There is a lack of forums for IT security to be discussed, and for CFIA IT Security to be made aware of the IT security practices within CFIA business lines, such as the Science or Operations Branches. Furthermore, responsibility for supply and care of these systems was to be transitioned from the Science Branch to the IMIT Branch, although this has not occurred. Some laboratories have fairly significant separate networks (e.g. up to 50 computers and one server) and proprietary software.

2.1.7 Recommendations

AAFC 1 - The Assistant Deputy Minister (ADM), ISB, in collaboration with the ADM, CMB, should ensure AAFC further defines roles and responsibilities between itself and SSC in relation to IT Security, and as part of that process update and formalize the Terms of Reference for IT Security - related Governance Committees.

AAFC 1
Management Response: Agree

Action Plan:
1.1 ISB DG Strategic Management Directorate (SMD), in collaboration with appropriate Shared Services Canada (SSC) DG counterpart(s), will review and document IT Security related roles and responsibilities.

Target Date for Completion:
June 30, 2015

1.2 ISB DG SMD, in collaboration CMB DG Asset Management and Capital Planning (AMCP), will update, formalize and obtain approval of the Terms of Reference for IT Security related governance committees in alignment with the action plan #1.1 to include appropriate SSC involvement.

Target Date for Completion:
September 30, 2015

Lead(s) Responsible: ADM ISB, DG SMD; ADM CMB, DG AMCP; SSC DG, Client Relationships & Business Intake

CFIA 1- The Vice President, IMIT, in collaboration with the Vice President, Corporate Management, should ensure that the IT security governance framework is strengthened, through a reinvigorated Security Program Management Committee (SPMC). CFIA should either leverage an existing operational-level committee, or establish a new committee, to ensure there is a forum for the discussion of IT security issues on a more tactical basis and that encourages collaboration between IT Security and areas such as Science and Operations, as well as SSC. This should include CFIA further defining roles and responsibilities between itself and SSC in relation to IT Security.

CFIA 1
Management Response: Management accepts the recommendation.

Action Plan:
1.1 Management will create an IT Security Governance framework that will specify how IT Security will be governed using the existing Governance committees and will seek opportunities with other existing committees where input can be provided by other relevant stakeholders, such as the Security Program Management Committee, on which other Branches participate.

Target Date for Completion:
March 2016

1.2 Internal governance within IMIT Branch will be strengthened, to ensure that IT Security will be engaged early in the project management process, so that risks can be identified and addressed.

Target Date for Completion:
March 2016

1.3 Management will continue to engage SSC in discussions aimed at further definition of roles and responsibilities of both parties.

Management will lead and/or participate in all appropriate Government of Canada fora that identify the processes for how SSC and Departments work in partnership in regard to IT Security.

Target Date for Completion:
Ongoing

Lead(s) Responsible:
VP, CMB; Vice President, IMIT; ED, Strategic Planning and Management

2.2 IT SECURITY RISK MANAGEMENT

2.2.1 The audit expected that AAFC and CFIA adhere to Treasury Board baseline security requirements as outlined in the Policy on Government Security. The Policy requires each Department / Agency to establish a security program for the coordination and management of departmental security activities, and the proper management of security requires the continuous assessment of risks and the implementation, monitoring and maintenance of appropriate internal management controls involving prevention (mitigation), detection, response and recovery.

Findings Specific to AAFC

2.2.2 The AAFC Departmental Security Plan (DSP) was completed in February 2012, and the plan is next scheduled to be updated and reissued in April 2015. The DSP is considered to be a foundational document with the Departmental Security Risk and Opportunity Register (DSROR) considered to be an evergreen document that captures security risks and opportunities. The basis for input into the DSROR is an annual Security Risk and Opportunities workshop held each fall.

2.2.3 Although a Security Risk and Opportunities workshop was held, and results briefed to senior management, a formal DSROR and accompanying work plan and formal prioritization and tracking of mitigation measures has not been developed. In addition to the workshop, the DSROR per the DSP is expected to be updated based on certain other triggers, including in response to risks identified in completed Threat and Risk Assessments (TRA). This has not occurred.

2.2.4 In addition to the DSROR, IT Security Risk Management (ITSRM) has its own more specific IT Security Risk Register that was last updated in June

2012. IT Security has indicated that the register is required to be refreshed as it has not been updated on an ongoing basis. It is not known at the time of the audit how these IT Risks will be reflected in the DSROR and ultimately the DSP.

2.2.5 AAFC and SSC are working together, at the initiation of AAFC, on addressing the Top 35 IT Security Controls list from Communication Security Establishment Canada (CSEC) related to AAFC controls. This list is not specifically connected to AAFC's IT Security Risk Register.

Findings Specific to CFIA

2.2.6 CFIA has developed a five year Agency Security Plan (ASP) in 2012 to cover 2012-13 to 2017-18, with the intent to refresh the document annually as required. The five year ASP was based on risk workshops conducted in 2010-11 that identified several risks. In January 2014, a presentation on the ASP indicated the following short-term actions related to IT security:

- Implement encryption of laptops;
- Develop a traveler's protocol; and
- Create business continuity plans.

2.2.7 IT Security weaknesses outlined by CFIA IT Security in a December 2013 'State of the Union' presentation to the Vice-President IMIT, identified items such as access control rules and processes and the integration of security requirements into the SDLC process, including ensuring appropriate sign off of risks by programs / IT systems. It was further noted that these issues were identified in over 10 previous TRAs conducted for the Agency.

2.2.8 A CFIA specific IT Security Risk Register for the prioritization and tracking of risks has not been developed, nor has the ASP been further updated subsequent to the input of the 2010-11 risk workshops. It is not known at the time of the audit how the ASP will be updated and how IT Risks will be reflected in the update to the ASP, including the risks now posed by the creation of SSC.

2.2.9 Recommendation

AAFC 2 / CFIA 2 - The AAFC ADM, ISB / VP, IMIT in collaboration with the AAFC ADM, CMB and CFIA VP, Corporate Management should ensure that a formal process is developed for IT Security to manage a single integrated-process that considers the identification, prioritization, and tracking of IT security risks for AAFC and CFIA, and that this process is a formal input into the overall Departmental / Agency Security Plan.

AAFC 2
Management Response: Agree

Action Plan:
2.1 ISB DG SMD, in collaboration with CMB DGs, will determine and document the inputs to the integrated process to ensure all sources of IT security risks are included.

Target Date for Completion:
Completed

2.2 ISB DG SMD will develop a formal process to manage a single method for the identification, consolidation, prioritization and tracking of IT Security risks. This action links to #7.2.

Target Date for Completion:
July 31, 2015

2.3 ISB DG SMD, in collaboration with CMB DG AMCP, will incorporate the latter process (item 2.2) as a formal input into the overall Departmental Security Plan (DSP) and is aligned with DSP schedule.

Target Date for Completion:
September 30, 2015

Lead(s) Responsible: ADM ISB, DG SMD; ADM CMB, DG AMCP

CFIA 2
Management Response: Management accepts the recommendation.

Action Plan:
2.1 Management will develop a formal process for identification of risks in a Centralized Risk Register. This process will identify how risks will be identified, prioritized, and tracked, and how it will be used in the newly established IT Security Governance framework. This will be completed leveraging existing Agency Risk Management processes, and will input the Agency Security Plan.

Target Date for Completion:
Draft model developed October 2015; Completion April 2016

Lead(s) Responsible:
Vice President, IMIT; ED, Strategic Planning and Management

2.3THIRD PARTY MANAGEMENT

2.3.1 The audit expected that AAFC and CFIA have developed formal processes to ensure IT security is considered during contracting and/or the development of agreements with third party vendors utilized for the delivery of IT services.

Findings Specific to AAFC

2.3.2 Although there are few instances in which AAFC utilizes private sector third parties as service providers for IT outsourcing and hosting, there are instances in which private sector contractors play a significant role in the development and maintenance of IT systems.

2.3.3 The AAFC IT Security Policy Section includes requirements for the contracting for IT Services. Furthermore, security activities undertaken by the DSO in 2012-13 included a development of a new AAFC Security in Contracting Standard, the development of a new IT Security annex for contracts, and the tracking of all Security Requirements Checklists (SRCLs) via a database.

2.3.4 At AAFC, the IM/IT Security and Supply Management Division is responsible to support all IM/IT managers in all their requests for professional services, and is intended to centralize and standardize all IM/IT procurements. Departmental Security Services (DSS) reviews all contracts for security requirements, and as required, consults with the ITSRM team.

Findings Specific to CFIA

2.3.5 CFIA utilizes a number of third parties as IT service providers, outside of SSC, the most significant being AAFC, which hosts CFIA's financial (i.e. SAP) and HR (i.e. PeopleSoft) systems. The audit found that there are agreements in place, and formal processes developed for ongoing communication, between CFIA and AAFC related to AAFC's hosting of SAP and PeopleSoft for CFIA.

2.3.6 CFIA utilizes third parties outside of government for some key Agency activities, this includes an organization that collects and manages livestock identification information on behalf of the Agency, and a number of third party laboratories that conduct sample collection and testing on behalf of the Agency. Agency information managed by a third party remains under the control of CFIA, and the Agency remains accountable to ensure the information is appropriately safeguarded.

2.3.7 There is no formally documented process through the contracting process to ensure IT Security is consulted or to ensure IT security is considered during the development of agreements or memorandum of understanding (MOU). Neither the MOU with the organization that manages livestock identification information or the sample contract reviewed with the third party laboratory included specific security requirements, other than a high level acknowledgement that the information would only be used for purposes that related to the agreement / contract. Neither document outlined the security incident and/or breach management process, or the processes related to the termination of the agreement / contract (e.g. retention and disposition of Agency information).

2.3.8 Although CFIA required both parties outlined above to agree to a right to audit clause, there is not any regular or formal assessments of the security controls utilized by the third parties.

2.3.9 Recommendation

CFIA 3 - The Vice President, IMIT, in collaboration with the Vice President, Corporate Management, should ensure that a formally documented process is developed that ensures IT Security is consulted in relation to agreements and contracts and that where required, third party adherence to security requirements is assessed and monitored.

CFIA 3
Management Response: Management accepts the recommendation.

Action Plan:
3.1 CFIA will use the existing PWGSC Industrial Security process for third parties as required to ensure that parties are accredited to the appropriate Facility Security Clearance (for classified information) level to manage Agency information within their establishment. PWGSC ensures that safeguarding requirements are adhered to through periodic audits as established by CFIA.

Security risks are further assessed through the Architecture Review Committee, which is currently being strengthened. CFIA has limited amounts of data that is held by third parties, but as it may be an area of growth in the future, assessments of contracted parties that process third party data on behalf of CFIA, will be considered as part of the Risk Assessment process.

Target Date for Completion:
Completed

3.2 The risk of third party data will be prioritized in the Centralized Risk Register.

Target Date for Completion:
October 2015

Lead(s) Responsible: Vice President, IMIT; ED, Strategic Planning and Management; VP, CMB

2.4 MANAGEMENT OF DIGITAL INFORMATION

2.4.1 The audit expected that AAFC and CFIA have implemented appropriate policies, procedures and tools for the management of sensitive digital information assets, and that this information is appropriately classified and safeguarded.

Findings Specific to AAFC

2.4.2 The management of sensitive digital information is a high priority for AAFC with extensive measures currently in place to mitigate the risks associated with using sensitive information. The findings identified by the audit team include opportunities to improve the existing measures.

2.4.3 AAFC has developed an IT Security Program Framework, including IT Security policies and user guidance, which covers key IT security related content, including at a high-level, the classification and safeguarding of sensitive digital information. AAFC has also worked with the Communications Security Establishment Canada (CSEC) on a Cyber Security project which included identifying those areas that manage classified information at AAFC.

2.4.4 AAFC is leveraging both internal networks and those of federal government partners for the processing and transmission of classified information. Within some program areas that handle a significant amount of classified data, there is a reliance on standalone laptops to process Secret information, with information shared between users on USB keys, and backed up on an external hard drive. Classified information is also processed and transmitted through less secure means, for example through the use of USB keys and within IT systems not accredited to process Secret information.

2.4.5 Protected information is not being formally classified or labelled in a consistent fashion throughout the Department. Many program areas, especially those in the regions and at research labs, are still utilizing

network drives to maintain at least some of their information, including protected information and information of a proprietary nature with intellectual property rights. Testing of access to these network drives indicated excessive access to the file shares. Furthermore, there were a significant number of SSC employees with administrative rights and AAFC was not able to validate if access by these SSC employees was appropriate.

2.4.6 USBs are used throughout the Department; and are not tracked or controlled in any formal or consistent fashion. AAFC has developed a Business Case that was approved for the Secure Use of Portable Storage Devices Project and a Project Charter and Project Management Plan has been developed. The intent of the project is to implement controls that are in line with the requirements of the May 2014 Treasury Board Secretariat (TBS) Information Technology Policy Implementation Notice on the secure use of portable data storage devices within the Government of Canada.

2.4.7 AAFC has developed a Defensive Travel Briefing: High Risk Travel process, and requires a mandatory security briefing for staff travelling for the Department outside of the country. As part of the process, staff can request 'loaner' laptops and mobile devices from ISB to be used while out of the country. Audit testing confirmed that those who had travelled outside the country during the audit period had undergone the mandatory security briefing. However, there is not a formal process in place for AAFC to easily track and monitor that 'loaner' IT equipment was requested and used by staff.

Findings Specific to CFIA

2.4.8 CFIA has implemented an IT Security Program Framework including the CFIA IT Security Directive and has developed guidance related to the identification, labelling, and safeguarding of Protected and Classified information. CFIA has developed an e-learning National Security Program, which includes a dedicated module on IT Security, which all CFIA employees are mandated to be taken by September 2015. Employees must then subsequently take a condensed version of the course each time they renew their ID cards every five years.

2.4.9 Through CFIA IT Security's assessment of the security classification of data within the Agency's IT systems, as of December 2013, IT Security estimated that at least half of the information within the Agency's systems was not appropriately protected. A major cause of this was noted as CFIA's network being accredited to only a Protected A standard.

2.4.10 The requirements to protect classified information are generally understood within the Agency, although the Agency lacks the appropriate tools to efficiently and effectively process and store classified (i.e., Secret) information through electronic means. Given this, examples were cited that Secret information may be emailed through a password protected document or transferred through unsecure USB keys.

2.4.11 Protected information is not being formally classified or labelled in a consistent fashion throughout the Agency, for example inspection reports and certain types of surveillance data were identified as being potentially sensitive (up to Protected B), and are not, as a general rule, labeled as such.

A significant amount of information is still managed through email and network drives, through audit testing it was determined this included not only Protected B information but very sensitive information related to investigations and enforcements that may be classified up to Protected C.

Through testing it was noted there was excessive access to network file shares. Furthermore, there were a significant number of SSC employees with administrative rights and CFIA was not able to validate if access by these SSC employees was appropriate.

2.4.12 There is no process for the regular review of security measures implemented by CFIA inspectors at establishments. For those establishments without a permanent inspector presence, IMIT staff noted that inspectors may plug their laptop directly into an establishment's network, which exposes the laptop to any risks related to the establishment's network, which may not be appropriately safeguarded.

2.4.13 CFIA has developed a travel security protocol that applies to staff travelling for the Agency outside of the country. As part of the protocol, staff members are provided a briefing, and may be provided 'loaner' laptops and mobile devices from IMIT to be used while out of the country. Implementation of the protocol has currently been ad hoc, and generally at the request of staff.

2.4.14 Recommendations

AAFC 3 / CFIA 4 - The ADM, ISB / VP, IMIT in collaboration with the AAFC ADM, CMB and CFIA VP, Corporate Management should ensure that procedures, training, and tools related to the identification, labelling, and management of classified (e.g. Secret) and protected information within the Department are developed and implemented to ensure compliance and improve awareness. This includes limiting the use of network drives for the storage of sensitive information.

AAFC 3
Management Response: Agree

Action Plan:
3.1 CMB DG AMCP will review and update departmental information classification guide and supporting documentation.

Target Date for Completion:
Completed

3.2 ISB DG SMD, in collaboration with CMB DG AMCP, will update IT Security Policy to ensure clarity on how Protected and Classified information can be processed using IT systems at AAFC and communicate the updated policy to managers and staff.

Target Date for Completion:
December 31, 2015

3.3 CMB DG AMCP will continue to promote the current web-based training course for AAFC staff which includes handling of Protected and Classified information (hard copy and electronic) and ensure the currency of related tools such as web content and awareness pamphlets. Furthermore, specific scenario-based training will be developed to address the handling of sensitive information (Protected and Classified documents). The Security Awareness training is mandatory at AAFC. In addition, all employees upon being granted or updated for their reliability status or security clearance must sign an "Acknowledgment of Understanding - Security Responsibilities Related to Protected and Classified Information" form, countersigned by their manager, which includes instructions on handling, transmission and packaging of both electronic and hard-copy Protected and Classified information.

Target Date for Completion:
Completed

3.4 ISB DG SMD with review and update the Statement of Sensitivity template which is used to classify information being processed by IT systems, to align with updated departmental information classification guide.

Target Date for Completion:
Completed

3.5 ISB DG SMD, in collaboration with ISB DG IMS, will review security of systems designed to process protected information and to expand their use in order to limit use of network drives for protected information.

Target Date for Completion:
September 30, 2015

3.6 ISB DG SMD, in collaboration with ISB DG Information Management Services (IMS), as directed by the Horizontal Management Committee (HMC) in alignment with GC and AAFC priorities, will implement systems for more secure processing of classified information and to reduce the reliance of shared drives for the storage of sensitive information.

Target Date for Completion:
December 31, 2015

Lead(s) Responsible: ADM CMB, DG AMCP; ADM ISB, DG SMD, DG IMS

CFIA 4
Management Response: Management accepts the recommendation.

Action Plan:
4.1 As the CFIA Network is not accredited to process Classified and Protected electronic information, alternative have been provided. A multi-year effort to strengthen mobile device security has been initiated, beginning with the implementation of hard drive encryption. Access has also been provided to existing government classified networks in the NHCAP facility, and stand-alone processing capability is provided to those areas of high risk. It should be noted that Shared Services Canada is responsible for the provision of a GoC Secure Network; however this capability is anticipated to take a few years. Until that time, CFIA will continue to use various solutions to ensure classified information is treated appropriately.

Target Date for Completion:
Ongoing

<u>Education and Awareness:</u>
4.2 Launched mandatory on-line learning modules for CFIA employees on the management of sensitive information.

Target Date for Completion:
Completed

4.3 Publication of guide to educate employees on procedures for identifying, labelling, transmitting and storing Protected and Classified

information. This guide will continue to be distributed during the Security Awareness Week campaign, posted on Merlin and provided to employees during Security Briefings.

Target Date for Completion:
Ongoing

4.4 Continue regular messaging from the Agency Security Officer to promote awareness for the security and protection of information with emphasis on compliance including the procedures for handling Classified information in a secure manner, off the network.

Target Date for Completion:
Ongoing

Compliance:
4.5 Continue with the Agency's recently implemented security sweep program to ensure employee compliance to appropriate management of Protected and Classified information.

Target Date for Completion:
Ongoing

Lead(s) Responsible: VP Corporate Management and CFO; Executive Director – ASMD; ED, Strategic Planning and Management

AAFC 4 - The ADM, ISB, in collaboration with the ADM CMB, should ensure that the high risk travel process includes the formal tracking of the use of 'loaner' IT equipment to allow DSS and ITSRM to monitor adherence to this aspect of the process.

AAFC 4
Management Response: Agree

Action Plan:
4.1 There is an electronic device (laptop, BlackBerry) 'loaner' program in place at AAFC for employees travelling abroad. CMB DG AMCP will provide, on a regular basis, reminders to all staff regarding travel responsibilities to increase awareness and remind them of the existing guidelines, procedures, and 'loaner' device program. These guidelines and procedures will be reviewed regularly to ensure they address the evolving security environment.

Target Date for Completion:

Completed

4.2 ISB Director IT Client Services will update the IT equipment travel 'loaner' process to include tracking utilization and providing Departmental Security Services (DSS) with access to this information.

Target Date for Completion:
May 15, 2015

4.3 CMB DG ACMP and DSS, in collaboration with ISB DG SMD and IT Security Risk Management (ITSRM) will update processes to include performing monthly monitoring of utilization of 'loaner' equipment and implement policy enforcement as required. Report on monitoring to Departmental Security Officer (DSO) and senior management on quarterly basis or as required.

Target Date for Completion:
July 15, 2015

Lead(s) Responsible: ADM SMD, DG AMCP; ADM ISB, Director IT Client Services

CFIA 5 - The Vice President, IMIT in collaboration with the Vice President Corporate Management, should ensure that adherence to the travel security protocol becomes mandatory for all staff within the Agency, and adherence to the process is monitored.

CFIA 5
Management Response: Management accepts the recommendation.

Action Plan:
Policy
5.1 Promulgate the Agency Travel Security Directive to provide employees with direction on travel security.

Target Date for Completion:
May 2015

5.2 Security and Accommodation Services and International Coordination Committee to identify travellers that require a Travel Security Briefing.

Target Date for Completion:
Completed

5.3 Security and Accommodation Services will conduct regular verifications of Agency travel request sources to ensure employee compliance with the Travel Security Directive.

Target Date for Completion:
Ongoing

Lead(s) Responsible: VP Corporate Management and CFO; Executive Director – ASMD

2.5 PHYSICAL SECURITY TO IT ASSETS

2.5.1 The audit expected that AAFC and CFIA would have implemented appropriate controls to ensure that physical access to sensitive information assets are appropriately restricted.

2.5.2 Although the transfer to ownership of larger data centres to SSC has taken place, AAFC and CFIA continues to be responsible for the actual granting of access to some of these locations.

2.5.3 For the data centre in one of the Regional / Area Offices used by both AAFC and CFIA, access is controlled by CFIA, given that there are no SSC personnel in the Region that support regional operations. SSC asked for access to the server room to be further restricted, resulting in the removal of access from some IT personnel; however, testing confirmed there remained excessive access.

2.5.4 AAFC and CFIA staff remain responsible for some of the smaller data centres / server rooms within AAFC research centres and regions, and CFIA district offices and laboratories.

Findings Specific to AAFC

2.5.5 For an AAFC research centre included in the audit, in which the data centre on site had not been transferred to SSC (i.e. smaller data centres), testing noted excessive access, as well as duplicate access cards that had not been deactivated. Based on a previous building and facilities assessment, an access card reader was installed for the server room to replace the former PIN pad system; however, the PIN pad system is still active and staff with knowledge of the PIN can bypass the card reader system. Staff could not recall the last time the PIN was changed. For an AAFC Regional Office, the general office area was restricted by access card, however, there were no further physical access controls in place to restrict access to the server room. Furthermore, the server cage was unlocked.

Findings Specific to CFIA

2.5.6 For a CFIA Area Office visited for testing, in which the data centre on site has been transferred to SSC, CFIA staff on site continue to manage the access card process. The audit found that due to access card system limitations, over half of those that had access to the server room did not require access. There were also several cards that were active but 'spares' reserved for contractors.

2.5.7 For a CFIA District Office included in the audit, in which the data centre on site had not been transferred to SSC, testing noted excessive access, as some access cards were either duplicate or unnecessary 'backup' cards.

2.5.8 For the CFIA laboratories included in the audit, access to the server room was restricted by a key, and a limited number of authorized staff had access. In order to gain access to the server room, an individual would first need to gain access to the laboratory building's themselves, which are restricted.

2.5.9 Recommendation

AAFC 5 / CFIA 6 - The ADM, ISB / VP, IMIT in collaboration with the AAFC ADM, CMB and CFIA VP, Corporate Management should engage SSC to ensure roles and responsibilities for the granting, and regular review, of server room access is formalized. Once this has been done, AAFC / CFIA can determine their responsibility to ensure appropriate controls are established to ensure adequate restriction of physical access to IT infrastructure.

AAFC 5
Management Response: Agree

Action Plan:
5.1 ISB Director of Client Services and CMB DG AMCP, in collaboration with SSC, will develop an inventory of AAFC physical locations that contain servers and related IT infrastructure and document current access control process, roles and responsibilities.

Target Date for Completion:
May 29, 2015

5.2 ISB DG SMD and CMD DG AMCP, in collaboration with SSC, will formally identify and agree to roles, responsibilities and procedures including oversight for access and control of all physical locations

identified to ensure adequate restriction of physical access to IT infrastructure.

Target Date for Completion:
September 30, 2015

5.3 ISB Director IT Client Services, in collaboration with SSC, will implement procedures as defined and will monitor and report on ongoing compliance to the Departmental Security Officer (DSO) and Chief Information Officer (CIO) as appropriate on a quarterly basis.

Target Date for Completion:
December 31, 2015

Lead(s) Responsible: ADM CMB, DG AMCP; ADM ISB, DG SMD, Director IT Client Services; SSC DG, Client Relationships & Business Intake

CFIA 6
Management Response: Management accepts the recommendation.

Action Plan:
Access Control Protocols
6.1 Identify a SSC representative with appropriate level of authority to review and approve access rights to SSC server rooms in CFIA space.

Target Date for Completion:
December 2015

6.2 Formalize agreement between CFIA and SSC which clarifies roles and responsibilities for the review, approval and granting of access rights to server rooms.

Target Date for Completion:
December 2015

6.3. Conduct regular review and updates of access lists to ensure that only authorized SSC employees are granted access to server rooms.

Target Date for Completion:
Ongoing

6.4 Establish a key control process to ensure that appropriate restrictions are in place to control and limit access to server rooms.

Target Date for Completion:
December 2015

Lead(s) Responsible: VP Corporate Management and CFO; Executive Director – ASMD

2.6 IT SECURITY RISK ASSESSMENT

2.6.1 The audit expected that AAFC and CFIA have developed formal processes for IT security risk management to ensure IT systems have incorporated appropriate IT security controls. CSEC published new guidance on the IT security risk management process, replacing the old certification and accreditation (C&A) process with a new Security Assessment & Authorization (SA&A) process. The purpose of certification / assessment is to verify that the security requirements established for a particular system or service are met and that the controls and safeguards work as intended. The purpose of accreditation / authorization is to signify that management has authorized the system or service to operate and has accepted the residual risk of operating the system or service.

2.6.2 There is a gap in AAFC and CFIA's IT risk assessment processes given SSC has not formally acknowledged the risks related to the IT infrastructure that is the responsibility of SSC. This results in action plans developed as part of the IT risk assessment process that do not include the risks and corresponding mitigation measures related to IT infrastructure.

Findings Specific to AAFC

2.6.3 AAFC established an SA&A framework in 2012 for which all new ISB systems and critical legacy systems must follow. Roles and responsibilities have been formally documented and the process has been incorporated into the Departmental IM/IT Portfolio Management Framework, and the System Development Life Cycle (SDLC). AAFC has completed the SA&A process for all critical systems, although a formal authorization to operate has not been obtained for all of these systems.

2.6.4 Through sample testing, the audit noted that for systems under development since the establishment of the SA&A framework, although SA&A activities such as Threat and Risk Assessments (TRAs) and Vulnerability Assessments (VAs) have been conducted, there has not been a formal follow-up on the mitigation of the risks identified. Furthermore, there was no documentation that could be provided to demonstrate that systems are taking a controls-based approach for IT security. For instance, there was no evidence of a 'catalogue' of security controls based on the system's security requirements that was then formally traced through a security requirements traceability matrix to the

implemented controls that was assessed through the TRA, and subsequently could be tested if applicable.

2.6.5 There is not a formal continuous monitoring and testing strategy in place, current monitoring consists of reviewing significant changes to systems for additional risks, which may require a formal assessment through an updated TRA. Of note, for critical systems, ITSRM has ensured they are made aware of any changes to the system through the formal Request for Change (RFC) and their attendance at Change Control Committee.

Findings Specific to CFIA

2.6.6 For CFIA, an enterprise project management office (ePMO) was created in April 2010 to develop an Agency wide approach for project management; however, there is no documented process or gates to ensure that IT Security is integrated into projects and initiatives. IMIT planning staff has recently developed a tracking and costing estimate sheet to track IT enabled projects and ensure that costs, including those for IT security, are included in project estimates.

2.6.7 A documented IT Risk Assessment does not exist within CFIA, nor has such a process been incorporated into the SDLC. IT Security has not been formally consulted on IT projects being undertaken for the Operations Branch. Risks identified in TRAs are often not formally mitigated or followed-up. Furthermore, there was no documentation that could be provided to demonstrate that systems are taking a controls-based approach for IT security. For instance, there was no evidence of a ‘catalogue’ of security controls based on the system’s security requirements that was then formally traced through a security requirements traceability matrix to the implemented controls that was assessed through the TRA, and subsequently could be tested if applicable. There is not a formal continuous monitoring and testing strategy in place. Technical Vulnerability Assessments (VAs) have generally not been performed.

2.6.8 Recommendations

AAFC 6 - The ADM, ISB should ensure that a formal authorization to operate is in place for all critical systems within the Department.

AAFC 6
Management Response: Agree

Action Plan:

ISB DG SMD, in collaboration with SSC, will ensure that formal authorization to operation is completed for all the outstanding AAFC critical systems by completing the remaining Security Assessment Reports and obtaining ADM level authorization from AAFC and SSC.

Target Date for Completion:
May 29, 2015

Lead(s) Responsible: ADM ISB, DG SMD; SSC DG, Client Relationships & Business Intake

AAFC 7 - The ADM, ISB should ensure that as part of the SA&A process, all new systems undertake a more formal security controls-based approach, and that risk identified during the initial assessment activities (i.e. TRA and VA) are followed up in a timely manner, prior to system 'go live', furthermore a more formal and comprehensive approach for the continuous monitoring of IT security risks and controls is developed.

AAFC 7
Management Response: Agree

Action Plan:
7.1 ISB DG SMD will update the Departmental IM/IT Portfolio Management Framework, templates and checklist and ensure that Project Managers and Directors are aware that formal security controls must be identified, used as input to system requirements, and approved by Investment Planning Committee prior to moving forward to the planning phase deliverables.

Target Date for Completion:
June 30, 2015

7.2 ISB DG SMD will update the Departmental IM/IT Portfolio Management Framework, templates, checklist and change control processes to ensure that the Project Managers and Project Directors are aware that assessment activities, including formal IT Security Authorization to ensure risks identified during the initial assessment phase are mitigated and formal authorization to operate are completed prior to system "go live".

Target Date for Completion:
June 30, 2015

7.3 ISB DG SMD will develop and implement a comprehensive and risk-based approach for continuous monitoring of IT Security Risks and controls throughout the lifecycle of systems.

Target Date for Completion:
July 31, 2015

Lead(s) Responsible: ADM ISB, DG SMD

CFIA 7 - The Vice-President IMIT should ensure that as a formal IT Risk Assessment process is established within the Agency and that all new systems undertake a more formal security controls-based approach that risks identified during assessment activities (i.e. TRA and VA) are followed-up in a timely manner, and a continuous monitoring strategy is developed. Existing critical systems should be revisited to ensure an authorization to operate is obtained and reevaluated on a periodic basis.

CFIA 7
Management Response: Management accepts the recommendation.

Action Plan:
7.1 Management will procure a senior consultant to provide recommendations toward creating the Risk Assessment approach based upon controls. All new systems are currently required to complete a Threat Risk Assessment. *Procurement of 7.1 is currently underway.*

***NOTE**: The time, scope and cost of items 7.2 – 7.4 below are dependent on the completion of item 7.1. therefore, target dates provided for these items are broad estimates only and subject to change.*

Target Date for Completion:
Completed

7.2 From this assessment, management will create a Risk Assessment program, where risks identified during assessment activities will be fed into the Centralized Risk Register for prioritization and assignment. Once this program is in place, all new systems will be subject to it.

Target Date for Completion:
April 2016

7.3 A continuous monitoring strategy will be developed in conjunction with the Risk Assessment program, of which the Centralized Risk Register will be a major contributing factor.

Target Date for Completion:
April 2016

7.4 A strategy to address and re-evaluate existing systems will be developed as part of the Risk Assessment program.

Target Date for Completion:
April 2016

Lead(s) Responsible: Vice President, IMIT; ED, Strategic Planning and Management

2.7 LOGICAL ACCESS CONTROLS

2.7.1 The audit expected that AAFC and CFIA have ensured that logical access to systems has been appropriately restricted to authorized users. The audit assessed logical access controls within AAFC and CFIA through a more detailed review of a number of IT systems. Controls related to the timely removal of the network access of employees were also reviewed.

Findings Specific to AAFC

2.7.2 At AAFC, the Employee Separation form is intended to be used throughout the Department to begin the termination process, although it was noted that regions often have their own form or may process a termination without a form. Once the separation form is completed by the terminated employee's manager and submitted, it is entered as a ticket into AAFC's ticketing system (and attached to the ticket), which generates additional tickets to inform the appropriate individuals to take specific action, such as disabling network access. Audit testing noted that the Active Directory (AD) account that provides access to the network was not disabled for some departed employees; in addition, many did not have a form on file. Although AAFC is responsible for disabling the network accounts of 'normal' end users, for those with administrative privileges to the network, the request to disable the account must be sent from AAFC to SSC. As part of the exit process described above, there is no formal process to ensure that this occurs.

2.7.3 The audit team selected a sample of non-critical AAFC systems to review logical access controls. Critical AAFC systems (such as SAP) were not included in the sample as similar IT Security audits are planned by external bodies such as the OCG and AAFC Internal Audit plans to conduct an audit focusing on SAP in 2015-16.

2.7.4 A formal process exists for the granting of user access to the IT systems; however, through audit testing a sample of new and modified user accounts, it was noted that exceptions were noted in that evidence that the formal process was followed was not on file.

2.7.5 None of the IT systems reviewed in detail as part of the audit have a formally documented process in place to regularly review user access.

2.7.6 Through a review of privileged access to the IT systems, the audit team concluded that privileged access was appropriate for two out of the three systems audited; however, access for users with the highest level of privilege in the system was not appropriate, this was based on either the user not having the appropriate security clearance or that they had transferred to another function.

2.7.7 Shared privileged accounts were identified in each IT system tested, although access to these shared accounts were appropriately restricted, there were no formal procedures to further control (e.g. password changes) or monitor the access and use of these accounts.

2.7.8 None of the systems had formal controls established to ensure an appropriate segregation of duties between security administration and the development and deployment of changes to the system.

Findings Specific to CFIA

2.7.9 The Departure from Agency form is intended to be used throughout the Agency to begin the termination process, although it was noted that regions often have their own form or may process a termination without a form. The form is intended to be completed by the employee and submitted to HR, where it is scanned and put into RDIMS. An email is then sent out from HR to the IT Service Centre indicating the departure with a RDIMS link to the Departure from Agency form. The IT Service Centre accesses the document from RDIMS, PDFs it and attaches it to a ticket which it generates. Testing noted that the Active Directory (AD) account was not disabled for some departed employees, and many did not have a form on file. Although CFIA is responsible for disabling the network accounts of ‘normal’ end users, for those with administrative privileges to the network, the request to disable the account must be sent from CFIA to SSC. As part of the exit process described above, there is no formal process to ensure that this occurs.

2.7.10 Related to password requirements, two of the four IT systems audited do not have defined requirements, in terms of complexity or password changes. Although one of the other systems does have password requirements, these were found to not be consistent with leading practice.

2.7.11 A formally documented process exists for the granting of user access for two of the four IT systems audited, while a process, although not formally documented, exists for the other two systems. Through audit testing,

exceptions were noted in that evidence was not on file that formal approval was given. None of the systems had a formal process to regularly review user access.

2.7.12 Through a review of privileged access to the applications, the audit team concluded that for three applications, some users with privileged accounts did not require this level of access. Shared privileged accounts were identified in each application, although access to these shared accounts were appropriately restricted, there were no formal procedures to further control (e.g. password changes) or monitor the access and use of these accounts.

2.7.13 It was noted that of the four IT systems selected for audit testing, all but one did not have formal controls established to ensure an appropriate segregation of duties between security administration and the development and deployment of changes to the system.

2.7.14 Recommendations

AAFC 8 / CFIA 8 - The ADM, ISB / VP, IMIT in collaboration with the AAFC ADM, CMB and CFIA VP, Human Resources should ensure that exit procedures and the adherence to them related to IT assets, are further formalized throughout AAFC / CFIA, including provisions to ensure the timely removal of network access.

AAFC 8
Management Response: Agree

Action Plan:
ISB Director IT Client Services, in collaboration with the CMB DG AMCP and CMB DG Human Resources (HR) will review, update and formalize current exit processes related to IT assets and will implement mechanisms, including communications to staff and management, to ensure they are followed including timely removal of network access.

Target Date for Completion:
June 30, 2015

Lead(s) Responsible: ADM ISB, Director IT Client Services; ADM CMB, DG Asset Management and Capital Planning, DG HR

CFIA 8
Management Response: Management accepts this recommendation.

Action Plan:

Management will initiate a review of the exit procedures and develop a strategy to improve timelines of completion, and adherence by all managers and employees.

Target Date for Completion:
October 2015

Lead(s) Responsible: VP, Human Resources

AAFC 9 / CFIA 9 - The ADM, ISB / VP, IMIT in collaboration with the AAFC ADM, CMB and CFIA VP, Corporate Management should ensure that standards for application logical access controls are reviewed and enforced, and adherence to these is reviewed through AAFC / CFIA's IT security risk management processes. This includes organizational-wide requirements for the granting and reviewing of user access, management of privileged accounts, and the appropriate segregation of duties.

AAFC 9
Management Response: Agree

Action Plan:
9.1 ISB DG SMD, in collaboration with the ISB DG IMS, ISB DG ADD, ISB Director IT Client Service and CMB DG AMCP will complete a review of application logical access standards and current practices update the standards to ensure appropriate account management processes including segregation of duties and, promote standards including training and communications to managers and staff.

Target Date for Completion:
September 30, 2015

9.2 ISB DG SMD will identify the specific security controls required for applications based on the standard updated in #9.1 and ensure that these controls are included in the baseline security controls for all applications moving forward.

Target Date for Completion:
December 31, 2015

9.3 ISB DG SMD, in collaboration with the ISB DG IMS, ISB DG ADD, and ISB Director IT Client Services will review all applications, starting with critical and high priority applications, to determine adherence to updated standards.

Target Date for Completion:
March 31, 2016

9.4 ISB DG SMD, in collaboration with the ISB DG IMS, ISB DG ADD and ISB Director IT Client Services, will update applications, where necessary, identified in# 9.3 to ensure that the necessary controls are implemented.

Target Date for Completion:
June 30, 2016

9.5. ISB DG SMD will assess bi-annually the application updates made to ensure that the controls implemented are in line with the standard, as per item #2.2.

Target Date for Completion:
September 30, 2016

Lead(s) Responsible: ADM ISB, DG SMD, DG ADD, DG IMS, Director IT Client Services; ADM CMB, DG AMCP

CFIA 9
Management Response: Management accepts this recommendation.

Action Plan:
Management will procure a senior consultant to develop a plan to address how application logical access controls are granted, reviewed, monitored and enforced. The plan will address the management of privileged accounts and the assurance of segregation of duties.

- *Completion of this is highly dependent upon securing appropriate funding for this initiative, and the successful progress of other Agency initiatives, such as RAMP.*

Target Date for Completion:
April 2016

Lead(s) Responsible: Vice President, IMIT; ED, Strategic Planning and Management

ANNEX A: AUDIT CRITERIA

Line of Enquiry 1:

A governance structure for IT Security has been established for the Department / Agency and its relationship with partners and third parties.

1.1 A governance structure for IT Security has been established and supported through an appropriate IT security framework.

- 1.1.1 Accountabilities, delegations, reporting relationships, and roles and responsibilities for IT security are defined, documented, and communicated to relevant persons.
- 1.1.2 Those charged with governance have clearly communicated mandates, are actively involved, have a significant level of influence, and exercise oversight of management processes.
- 1.1.3 The oversight body meets regularly and reviews information related to IT Security priorities and plans, provides advice on issues, reviews performance of the IT security function, and communicates its decisions to the organization in a timely manner.

1.2 AAFC / CFIA have defined the governance, reporting, and communication requirements related to its relationship with Shared Services Canada.

- 1.2.1 IT security roles and responsibilities of SSC have been formally defined, documented, and communicated.
- 1.2.2 A service level agreement with SSC exists and includes defined service levels for IT security services and adherence to these requirements is monitored.
- 1.2.3 Governance mechanisms are in place to ensure regular communication and review of information related to IT security services provided by SSC.

1.3 A formal relationship with third party vendors other than SSC for the delivery of IT services exists and governance mechanisms are in place to ensure defined business objectives are met.

- 1.3.1 A formal process for the selection of third party vendors other than SSC for the delivery of IT services is in place and includes consideration of IT security requirements.
- 1.3.2 Third party vendor agreements for vendors other than SSC include IT security requirements and adherence to these requirements is regularly reported, monitored, and assessed.

Line of Enquiry 2:

A formal process for the management of sensitive information assets exists and is consistently implemented to ensure the appropriate classification, use, and management of sensitive digital information.

2.1 A formal process for the management of sensitive digital information assets exists and is consistently implemented to ensure the appropriate classification, use, and management of sensitive digital information.

- 2.1.1 Formal policies and procedures have been developed, and appropriate tools provided, related to the management of sensitive digital information assets.
- 2.1.2 Physical security processes are in place and implemented to ensure that physical access to sensitive information assets are appropriately restricted.

Line of Enquiry 3:

A formal process for IT security risk management is in place and implemented for IT systems.

3.1 A formal process for IT security risk management is in place and implemented for IT systems.

- 3.1.1 The SA&A process has been defined, documented, and communicated and incorporated into the system development life cycle.
- 3.1.2 IT systems have been formally accredited and certified.
- 3.1.3 IT system design / architecture is documented and implemented based on appropriate security controls.
- 3.1.4 Comprehensive operation security documentation has been developed that is applicable to the IT system.
- 3.1.5 Continuous monitoring, assessment, and authorization maintenance activities have been implemented, and appropriate actions taken based on the results of these activities.

Line of Enquiry 4:

Logical access to systems is appropriately restricted to authorized users.

4.1 Logical access to systems is appropriately restricted to authorized users.

- 4.1.1 Logical security parameters are configured for user accounts to provide for user accountability and restrict unauthorized access.
- 4.1.2 Requests for access to systems follow a formal process, are made by user management, approved by system owners, and in line with business needs.
- 4.1.3 A formal employee off boarding process includes the return of all information assets and the removal of all access rights from information systems.
- 4.1.4 User access is regularly reviewed and changes to user access permissions are made in a timely manner.
- 4.1.5 Privileged user access is appropriate and restricted based on business needs.

ANNEX B: ACRONYMS

AAFC	Agriculture and Agri-Food Canada
AD	Active Directory
ADD	Applications Development Directorate
ADM	Assistant Deputy Minister
AEB	Audit and Evaluation Branch
AMCP	Asset Management and Capital Planning
ASO	Agency Security Officer
ASP	Agency Security Plan
CFIA	Canadian Food Inspection Agency
CFO	Chief Financial Officer
CMB	Corporate Management Branch
CSEC	Communication Security Establishment Canada
DG	Director General
DSO	Departmental Security Officer
DSMC	Departmental Security Management Committee
DSP	Departmental Security Plan
DSROR	Departmental Security Risk and Opportunity Register
ED	Executive Director
HMC	Horizontal Management Committee
HR	Human Resources
IMIT	Information Management and Information Technology
IMS	Information Management Services
ISB	Information Systems Branch
IT	Information Technology
ITSC	Information Technology Security Coordinator
ITSRM	Information Technology Security Risk Management
ITSWG	IT Security Working Group
NHCAP	National Headquarters Complex for the Agriculture Portfolio
OAE	Office of Audit and Evaluation
OAG	Office of the Auditor General
PGS	Policy on Government Security
PWGSC	Public Works and Government Services Canada
RDIMS	Record Document Information Management System
SA&A	Security Assessment and Authorization
SDLC	System Development Life Cycle
SISC	Security and Identity Steering Committee
SMD	Strategic Management Directorate
SPMC	Security Program Management Committee
SRCL	Security Requirements Checklists
SSC	Shared Services Canada
TRA	Threat and Risk Assessment
VA	Vulnerability Assessment