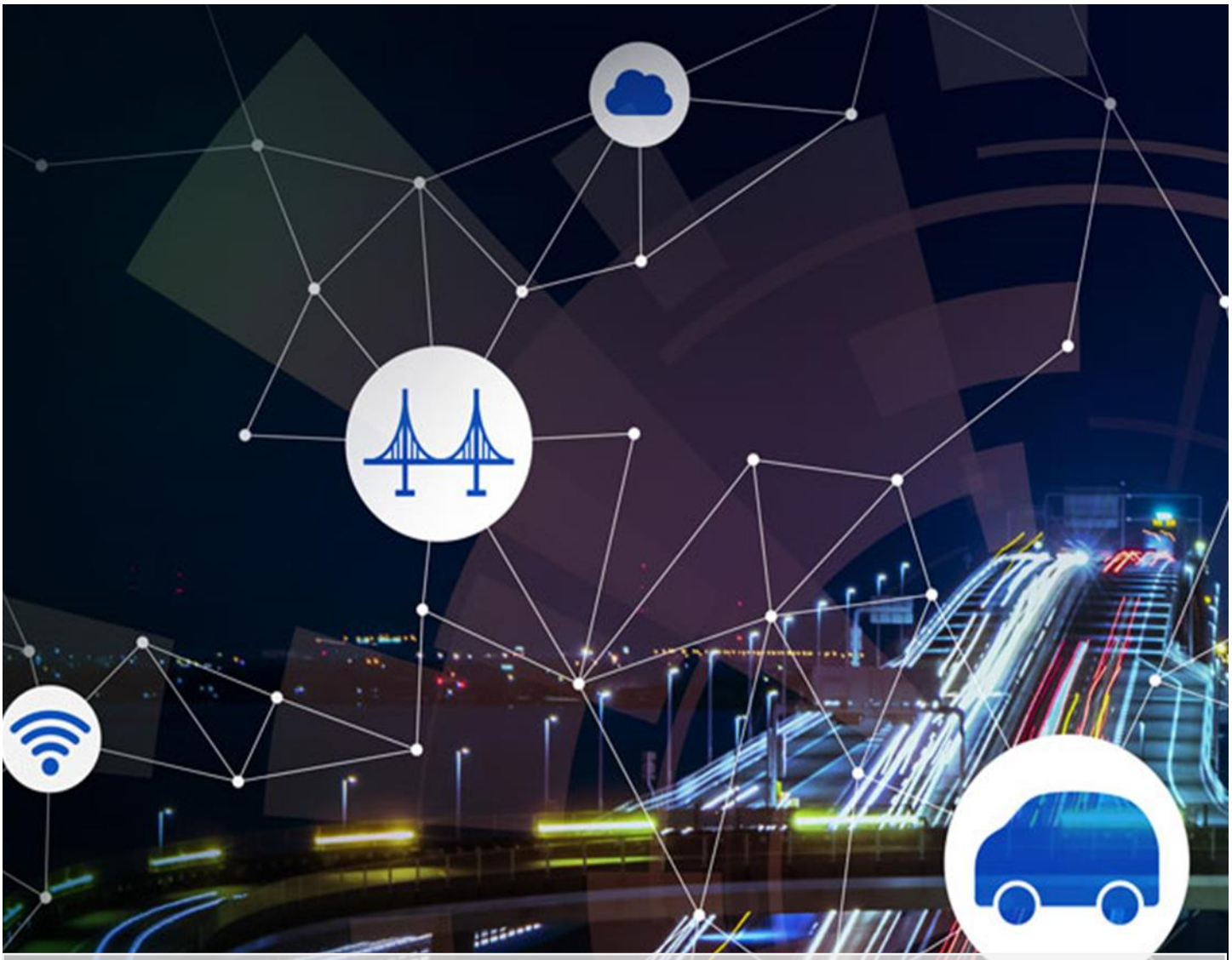

Infrastructure Canada – Internal Audit

Audit of Departmental Security

Final Report

October 7, 2019

Canada

Table of Contents

1. Executive Summary

Audit Objective

The objective of this audit was to assess the effectiveness of the departmental security program at Infrastructure Canada, as well as its compliance with the 2009 Treasury Board of Canada (TB) *Policy on Government Security* (PGS) and other relevant policies, directives and standards.

Why is it important?

INFC relies heavily on people, assets and information for the delivery of its programs and services. A breakdown in physical security in the form of unauthorized access to a facility could result in threat of violence to employees, loss of valued physical and information assets and compromise the continued delivery of key INFC services.

INFC had a workforce of approximately 593 people at March 31, 2019, working in four different locations in Ottawa and Montreal. INFC's assets include office furniture, vehicles and IT equipment, as well as fixed assets (such as land, bridges, and highway infrastructure) related to the New Champlain Bridge Corridor (NCBC) project. For the purpose of this audit the NCBC project assets were excluded from the scope, as those are managed by a private partner under a long-term public-private partnership agreement. INFC holds a large amount of electronic records, of which the majority is Unclassified or Protected A.

Strengths

INFC is taking advantage of the ongoing revision to the TB policy suite to update and streamline its departmental security policies and directives. As well, INFC will adjust the Terms of Reference to its existing governance structure to comply with the new security policy instruments. Now that the TB policy instruments are in effect (as of July 1, 2019), it is important for INFC to develop a timeline to complete the updating exercise in order to be fully compliant.

There are adequate physical security controls in place for the identification of physical assets, personnel security screening, identification badges, zoning and the storage, disposal and destruction of IT media.

A comprehensive security awareness program including training, computer pop-ups, posters, e-mails and guidance documents is in place.

INFC has a well-functioning Project Management Framework in place that includes security controls in the various phases of project development.

An up-to-date and tested Business Continuity Plan (BCP) in compliance with the TB Operational Security Standard for the BCP Program is in place.

Areas for improvement

Security risk management: A link between the Departmental Security Plan (DSP) and the Corporate Risk Profile exists; however, there is no formal risk register to ensure all key security risks are identified, assessed and mitigated.

Communications Security Establishment's Top 10 IT Security Actions: While taking some actions directly in support of the CSE's Top 10 security actions for which it is responsible, INFC has not

performed a formal cyber security assessment against the Communications Security Establishment's Top Ten IT security actions[1].

Addressing non-compliance with security policies and directives by INFC employees: At the time of the audit, 55%[2] of staff had taken the mandatory security awareness course, but recent security sweeps continue to reveal a large number of security violations. Furthermore, there was no correlation between employees who had taken the course and those found to have a security violation during the February 2019 security sweep.

Policy compliance: Most Information Technology (IT) systems at INFC, especially Legacy systems are operating without a valid Security Assessment and Authorization (SA&A) report required by the TB PGS. The SA&A process would have helped identify weaknesses noted during the audit in the areas of privileged account management and IT continuity planning. New systems (i.e. IRIS and GCdocs) introduced over the past year migrated in production with an interim authority to operate.

Security incidents: Not all security incidents are properly identified, recorded, assessed, mitigated and reported.

Inventory control of electronic equipment: There is a new inventory system in place to record all IT items; however, there is no periodic physical inventory taken and the records contain a number of items such as laptops, tablets and USB keys with unknown locations and owners.

Conclusion

Moderate improvements are required for INFC to have a well-defined and fully effective departmental security program in compliance with the TB PGS and other relevant policies, directives and standards. The most important challenge faced by INFC is the cultural change that will be necessary to move to a more security-conscious organization, and to implement the new TB PGS and other relevant departmental policies, directives and standards going forward.

Recommendations

A complete list of recommendations can be found in Section 7: Management Response and Action Plan.

[1] https://cyber.gc.ca/en/guidance/top-10-it-security-actions-protect-internet-connected-networks-and-information-itsm10189
[2] As of March 31, 2019 67% of employees had taken the training.

2. Background

The 2009 Treasury Board of Canada (TB) Policy on Government Security (PGS) is an essential component of the Government of Canada's national security framework. It establishes the responsibilities of deputy heads to help ensure that government Information, assets and services are protected against compromise and that individuals are protected against workplace violence. Now that the TB policy instruments have been finalized and are in effect (as of July 1, 2019), INFC's governance structure will be adjusted to comply with the new security policy instruments.

3. Audit Approach

3.1 Audit objectives and scope

The overall objective of the audit was to assess the effectiveness of the departmental security program at INFC, as well as its compliance with the 2009 TB *PGS* and other relevant policies, directives and standards. Specifically the audit sub-objectives assessed whether:

- There was an effective governance structure in place that supports transparent planning and decision-making related to departmental security.
- There were sufficient and adequate departmental security controls and processes in place to support security for individuals, facilities, physical assets, information management, and IT systems.
- The Department had in place a Business Continuity Planning Program (BCP) that supports the continued availability of services and their associated assets and resources.

The audit examined only the security activities under the responsibility of INFC. The scope of the audit was limited to the security aspect of physical assets, information management, and project management. The audit team examined communications between INFC and other partners (such as Shared Services Canada {SSC}), but excluded a direct review of their systems and practices. The INFC project assets such as the new Champlain Bridge were also not included in the scope of the audit. The audit work was conducted in Ottawa, but included a site visit to the Montreal office.

3.2 Approach and methodology

The audit engagement was conducted in accordance with the TB *Policy on Internal Audit* (eff. April 1, 2017) and the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing.

The audit engagement included various tests, as considered necessary, to provide reasonable assurance on the management of the departmental security program. These tests included, but were not limited to:

1. Conducting interviews with personnel with respect to the management of departmental security and related activities;
2. Reviewing applicable TB and departmental policy instruments and procedures for the management and administration of the Departmental Security function; and

3. Reviewing supporting documentation, attendance at meetings, process walkthroughs, and analytical review.

The conduct phase of this audit was substantially completed on March 29, 2019.

3.3 Risk assessment

As part of the preliminary planning process, a risk-based approach was used to establish the objectives, scope, and approach for this audit engagement. The approach included interviews with personnel and the review of important documents. A summary of the key inherent risks taken into consideration include the following:

There is a risk that…

- Insufficient executive management support and direction for departmental security may result in stakeholders not fully understanding or committing to security issues;
- Information management systems and practices are insufficient or not working as intended resulting in the security of INFC information being compromised;
- Physical security controls are not in place or working as intended resulting in facilities, personnel, assets and information not being adequately protected;
- Insufficient business recovery controls to support business interruptions may prevent timely resumption of INFC activities;
- Insufficient controls to manage security incidents may result in these not being detected, reported, investigated or resolved in a timely manner;
- Insufficient controls to manage security risks may result in INFC being exposed to those that exceed its risk appetite; and
- Insufficient or inadequate security awareness activities may result in unnecessary exposure that could damage the reputation of INFC.

3.4 Audit criteria

Taking into account these inherent risks, detailed audit criteria were developed. The criteria guided the audit field work and formed the basis for the overall engagement conclusion. The audit findings presented in the next section are aligned to individual criterion.

Please refer to Annex A for the detailed audit criteria.

4. Key Findings[3]

4.1 Governance

Sub-objective: To determine whether there is an effective governance structure in place that supports transparent planning and decision making related to departmental security.

Policies, directives and guidelines

Criterion: Complete, approved and up-to-date policies, directives and guidelines exist for departmental security.

The main security policy instruments at the time of the audit were the TB PGS (2009) and the INFC Departmental Security Policy (2007), both of which were outdated. The TB policy suite reset of the security policy architecture was approved by TB ministers on April 12, 2019 and came into effect on July 1, 2019.

The Treasury Board Secretariat (TBS) complemented the security policy with directives, standards and guidelines and INFC is taking advantage of the TB policy suite reset to streamline and update its own departmental security directives and guidelines. While much work has been completed within the INFC security policy suite, some tasks still need to be completed.

In conclusion, security policies for INFC are in place but need to be updated and approved. Establishing a timeline to complete this work, including departmental approval would support INFC's security program and ensure compliance with the updated TB policy suite.

Roles and responsibilities

Criterion: Roles and responsibilities for managing the departmental security program should be well established, communicated and assumed.

At INFC, responsibility for departmental security falls within the Information Management & Information Technology (IMIT) Directorate of the Corporate Services Branch. The IMIT Directorate comprises two divisions: Application Services, and Operational Support, security and Information Management (which includes the security group).

The Departmental Security Officer (DSO) is responsible for managing the departmental security program and reports functionally to the Deputy Minister (DM).. The DSO's roles and responsibilities are well-defined in the Government of Canada and INFC security policy instruments. To better describe and understand security roles and responsibilities at INFC, the audit team developed, with input from the Chief Information Officer (CIO) and the DSO, a RACI[4] chart in Annex B.

The current security roles and responsibilities are aligned with the existing TB policy instruments. Changes to the governance structure will be required to comply with the new PGS and *TB Directive on the integrated management of service, information, IT, and cyber*

[3]See Annex C for a scorecard with a summary of ratings and a conclusion for each criterion.

[4] RACI is an acronym for **R**esponsible, **A**ccountable, **C**onsulted and **I**nformed. A RACI chart is a matrix of all the key activities or decision-making authorities in an organization set against all the people or roles.

security. For example, the new *TB* PGS requires the DM to designate a Chief Security Officer, to replace the DSO position under the current PGS and provide leadership, coordination and oversight for departmental security management activities. The new *TB Directive on the integrated management of service, information, IT, and cyber security* requires the creation of a departmental Architecture Review Board to review and approve the architecture of all departmental IT services. The CIO has indicated that discussions of the required changes with INFC senior management are well underway.

In conclusion, the DSO's roles and responsibilities are defined and supported by clear authorities. Adjustments to the INFC governance structure is required with the recent approval of the new *TB Policy on Government Security* and *TBS Directive on the integrated management of service, information, IT, and cyber security.*

Communication

Criterion: A communication strategy is in place to ensure that employees are informed of their security roles and responsibilities.

As required by the TB PGS, INFC developed and approved a Departmental Security Plan (DSP), which outlines security risks and related security controls, a three-year action plan, and roles and responsibilities pertaining to performance reporting. The INFC DSP is the primary document for communicating security roles, responsibilities and accountabilities at INFC.

While the DSP is not distributed to all employees, it is presented to both the Investment Management Committee and Departmental Management Committee, and approved by the DM and shared with TBS. The DSP is a useful tool to communicate the current security posture and future security initiatives of the organization. The Policy is easily accessible to staff on the departmental INFRAnet site and a pop-up message appears at computer start-up to encourage staff to consult the IMIT policies. The DSP is complemented by the Security Sweep Directive and several resources such as the Clean Desk Guidelines and a user guide for encrypted USB keys. All staff are briefed on their security roles and responsibilities during the onboarding process at INFC and all employees are directed to take the mandatory security awareness course within one month of joining INFC.

In conclusion, there are several communication tools and activities in place to ensure that employees are informed of their security roles and responsibilities.

Risk management

Criterion: Security risks are systematically identified, documented, assessed and mitigated.

In a dynamic and complex public sector context, risk management plays an important role in strengthening government capacity to respond actively to change and uncertainty by using risk-based information to make decision-making more effective. The demonstrated ability to identify, assess, communicate and manage security risks builds trust and confidence, both within INFC and the government at large.

The TB PGS identifies security risk management as one of its core messages and notes that the management of security requires the continuous assessment of risks, this includes the implementation, monitoring and maintenance of appropriate internal management

controls involving prevention, detection, response and recovery. The associated TB *Directive on Departmental Security Management* states that the DSO is responsible for developing, documenting, implementing and maintaining processes for the systematic management of security risks. This will ensure continuous adaptation to the changing needs of the organization and the evolving threat environment.

The 2018-2021 INFC DSP describes the security risks that have been determined to hold the most potential for adversely affecting the ability of INFC to fulfill its mandate. It provides an alignment and linkage between the Corporate Risk Profile (CRP) and the associated security risks. For example, the 2019-21 CRP, under the Governance and Management risk category, states that the current operating model may no longer serve the new and evolving needs of the organization and could impact INFC's ability to leverage its functional areas in stewardship. An associated security risk statement specifies that process failures to adequately screen employees may result in unreliable individuals gaining access to sensitive INFC information and to the facility. Another security risk statement is that information may be compromised by negligence or by the deliberate unauthorized disclosure by an employee, which could cause embarrassment to INFC.

To identify security risks, INFC performed a security risk assessment by examining the previous and current versions of the DSP, CRP, and Threats and Risks Assessments (TRAs) of INFC facilities. For each security risk identified, related existing security controls were identified and residual risk was determined.

INFC does not maintain a departmental security risk register (or other tool) to systematically identify, assess, mitigate or accept residual security risk. A risk register should be used to review and report any residual security risk that exceeds established authorities for acceptance. There are a number of known security risks that are not documented and for which the residual risk is not formally accepted by management or compensating controls implemented. These include:

- Some staff have access to information exceeding their security clearance;
- Classified information in excess of Protected A is stored in shared network drives without additional protection;
- Recent security sweeps have disclosed security violations, many of which include not adequately protecting classified information; and
- A network Vulnerability Assessment (VA) in 2017 revealed a number of vulnerabilities that remained to be addressed at the time of the audit.

INFC has conducted TRAs for its four locations (180 Kent and 427 Laurier in Ottawa, as well as 800 René Lévesque and the site office in Montreal) within the last two years to ensure that INFC personnel remain safe and secure within INFC facilities, and that key INFC tangible and information assets are secure at an appropriate level. Several areas of concern were discovered during the TRAs for which recommendations were made and an action plan prepared.

INFC has eighteen IT applications in its application portfolio (Annex E), such as the Project Information Management System (PIMS) and Infrastructure Recipient Information System (IRIS). Of those eighteen, fifteen have not gone through the SA&A process. The three that have gone through the process received only Interim Authority to Operate (IAO) because they contain deficiencies in excess of the target acceptable risk of ''Low''. The IAO for the

Shared Information Management System for Infrastructure (SIMSI) expired in September 2016 and has not been extended. Without going through the certification process, there is no way of knowing if these applications contain vulnerabilities in excess of the residual risk acceptable to INFC.

The Communications Security Establishment (CSE), whose mission is to provide and protect information of national interest through leading-edge technology, issues a Top 10 IT security actions list to protect internet connected networks and information.

CSE's Top 10 IT Security Actions to Protect Internet Connected Networks and Information[5]:

Rank	Action	Responsibility (INFC, SSC or shared)
1	Consolidate, monitor and defend Internet gateways	SSC
2	Patch operating systems and applications	SSC
3	Enforce the management of administrative privileges	SSC/INFC
4	Harden operating systems and applications	SSC/INFC
5	Segment and separate information	SSC/INFC
6	Provide tailored awareness and training	INFC
7	Protect information at the enterprise level	SSC/INFC
8	Apply protection at the host-level	SSC
9	Isolate Web-facing applications	SSC
10	Implement application whitelisting	SSC/INFC

[5] https://cyber.gc.ca/en/guidance/top-10-it-security-actions-protect-internet-connected-networks-and-information-itsm10189

Although most of the IT security actions are related to the IT infrastructure and are the responsibility of SSC, there are a number of actions that are shared between SSC and INFC, or under the responsibility of the department. For example, INFC is responsible for minimizing the risk related to the number of users with administrative privileges for its applications and to conduct technical VAs for its applications to detect vulnerabilities in them.

The DSP includes a three-year action plan listing security activities, measures and controls to further reduce residual risks. However, given the lack of risk register, it is unclear whether these actions are required to respond to a residual risk that exceeds management risk tolerance or gaps observed to meet policy requirements.

In conclusion, security risk management practices need to be strengthened at INFC. Failure to effectively identify and manage security risks can result in sensitive INFC information being compromised by negligence or deliberate unauthorized disclosure by an employee, or a malicious actor may gain access to sensitive information, all of which could cause embarrassment to the Department. Alternatively, resources may be placed to mitigate risks well below management's tolerance level.

While it has taken some action directly related to the CSE's Top 10 security actions for which it is responsible, INFC has not performed a formal cyber security assessment against the Top Ten list. While not mandatory, such an assessment and corresponding remedial actions would help reduce the risk of exposure to cyber-attacks and other threat activities.

Recommendation #1:

It is recommended that the ADM, Corporate Services, in consultation with the DSO develop and implement a process to ensure that all key security risks are identified, assessed and managed. This includes assessing performance against the Communications Security Establishment's Top Ten security actions for which the department is responsible, to ensure alignment with best practices to protect INFC's networks and information.

4.2 Security controls

Sub-objective: To determine whether there are sufficient and adequate departmental security controls and processes in place to support security for individuals, facilities, physical assets, information, and IT systems.

Access controls

Criterion: Access controls are implemented and reviewed periodically to protect facilities and IT systems.

Physical access controls

The TBS *Operational Security Standard on Physical Security,* last modified in February 2013, requires that all departments control access to restricted areas using safeguards that will grant access only to authorized personnel and visitors in a manner that does not contravene safety requirements.

INFC recently conducted TRAs for its four locations to assess the physical security of each. The TRAs documented existing security safeguards, such as access card readers, door hardware, stairwell access, elevator access, Closed-Circuit Video Equipment (CCVE) cameras and parkade security.

The four TRAs included a number of recommendations to assist INFC in establishing a more robust security posture, which refers to the security status of an organization's networks, information and systems and to ensure that personnel remain safe and secure while working at INFC locations. None of the security risks identified were classified as a "show-stopper". Several of the risks identified were related to the fact that INFC is housed in privately owned buildings with commercial spaces located on the lower levels. For example, INFC could not decide to lock down the ground floor during a shelter-in-place event.

[redacted][6]

In conclusion, INFC has recently reviewed physical access controls for all its locations and it is adequately managing the risks identified.

IT access controls

The audit focused on controls related to user access management with special attention to the management of privileged accounts[7] for INFC applications.

User access management is the process of managing who has access to what information over time. It is more than an IT function, as this process affects every business function and

[6] Please note the audit has been processed in accordance with the *Access to Information Act* and certain information has been withheld from disclosure in accordance with exemptions in the **Act**

[7] A privileged account has more privileges than ordinary user accounts. Privileged accounts might, for example, be able to install or remove software, upgrade the operating system, or modify system or application security configurations.

every IT system user in the Department. While SSC is responsible for the management of access controls for many of INFC's IT systems such as e-mail and the network, INFC is responsible for managing access rights for its own applications. INFC is also responsible for reviewing the list of authorized users for IT systems not under its responsibility to ensure the access management at INFC is based on the least-privileged and need-to-know principles.

There is no process at INFC to periodically review user access lists and their privileges. Such a review would identify users that have left the organization or have changed responsibilities and no longer require access to parts of the system. This process would also help to identify generic accounts or users with privileged accounts that are no longer required. A review of user accounts has not been done for several years. This is important because a weakness in IT access controls could cause an inadvertent exposure which could result in loss or compromise of sensitive information, resulting in embarrassment for the Department.

User access controls were tested for three of the eighteen INFC applications. Access control weaknesses were noted for each, including the use of a generic super user account.

Recommendation #2:

It is recommended that the ADM, Corporate Services, in consultation with the Director, Applications Services, conduct periodic reviews of user accesses to INFC's IT systems with a focus on users with privileged and administrative access rights.

Security awareness

Criterion: A security awareness program is in place to guide individuals and ensure that they understand and comply with their security responsibilities and do not unintentionally compromise security.

The primary objective of a security awareness program is to educate employees on their responsibility to help protect the confidentiality, availability and integrity of INFC's information and information assets. Consequently, information security is everyone's responsibility, not just that of the security division.

At INFC, a comprehensive and up-to-date security training and awareness program is in place, including a security briefing during onboarding, INFRAmation articles, security tips, security guidelines, security posters, and security sweeps. Staff are also required to take the Canada School of Public Service A230 security awareness course within the first month of arrival at INFC.

If employees have a solid understanding of departmental security policies, procedures and best practices and comply with them, it can help protect an organization against hacktivists and cyber-criminals that scour the Web in search of targets and vulnerabilities. Moreover, it can reduce the risk and exposure to data integrity attacks and other threats.

Despite the security training and awareness program, there is a problem of non-compliance with security policies and directives by INFC staff. During the February 2019 security sweep, 41% of the 135 offices swept were not in compliance with TB's PGS and INFC's *Departmental*

Security Sweep Directive. Infractions found included unsecured documents (Protected A, Protected B, Protected C, Confidential, and Secret) and laptops with BitLocker[8] default Personal Identification Number (PIN[9]). This is important because end users are considered one of the weakest links in the cybersecurity chain. However, the audit team was informed by IM/IT security services that during the security sweep on June 25, 2019, the trend of violations had reduced significantly, as 88% of the 149 offices swept were in compliance.

At the time of the security sweep in February 2019, 55% of staff had taken the mandatory security awareness course. As of March 31, 2019, the number had climbed to 67%, still far short of the requirement of 100%. The security course has been part of INFC's mandatory training for several years and it is unclear why approximately a third of employees have not yet taken it. Furthermore, analysis revealed that there was no correlation between the employees who took the course and those found to have a security violation during the February 2019 security sweep. Although the course provides a good overview of security, it does not seem to be effective in reducing security violations.

The CSE's top 10 IT Security Actions includes providing tailored awareness and training. "Organizations should initiate regular awareness activities to address current user-related vulnerabilities and proper user behaviours. IT security awareness programs and activities should be frequently reviewed, maintained, and made accessible to all users who have access to organizational systems. Although system safeguards are expected to curtail suspected malicious activity on networks, the human element will continue to provide a risk of exposure. Current examples of spear phishing or improper handling of removable media shows the continued need to focus awareness in this area. In addition, regular reports to management on attempted or actual compromises will help to reinforce the behavioural changes needed. Management involvement in information protection decisions is essential when choosing appropriate security controls."

In conclusion, while efforts have been made to promote security awareness and training, improvements are needed to encourage employees to comply with their security responsibilities. Potential consequences may include reputational harm to INFC and employees. It is important to educate personnel on these potential negative impacts to INFC.

Recommendation #3:

It is recommended that the ADM, Corporate Services, in consultation with the DSO, review and revise awareness initiatives to ensure key risk areas, including compliance with the clean desk policy, are adequately communicated to INFC employees, and tested for effectiveness.

[8] BitLocker is the software tool used to encrypt the data on laptops, desktops and tablets.

9 A PIN is a number allocated to an individual and used to validate electronic transactions.
9

Recommendation #4:

It is recommended that the ADM, Corporate Services, in consultation with the DSO, establish and periodically report to senior management and the DM on metrics related to the security culture at INFC, such as statistics on infractions found during security sweeps.

Incident management

Criterion: There is an effective process to identify, monitor, analyze, assess and report security incidents in a timely manner.

The TB PGS defines a security incident as "Any workplace violence toward an employee or any act, event or omission that could result in the compromise of information, assets or services." There are two major categories of security incidents: security violations and security breaches. A security violation is the act of violating a security policy or procedure that may lead to the compromise of sensitive information or assets. For example, INFC conducts routine security sweeps to verify compliance with government and departmental security policies and procedures, and may detect security violations. A security breach is an act of omission, deliberate or accidental, which results in an actual compromise such as the loss of an unencrypted USB key containing sensitive information. It is important to report security violations in a timely manner so that corrective action can be taken before a security breach or serious security incident occurs.

The current incident management process is documented in the 2007 INFC Departmental Security Policy. It requires that all security incidents, including both violations and breaches, be reported to the DSO for investigation and to ensure that thorough records are maintained. Two generic security mailboxes, Security Services and IT Security Services have been created for INFC staff to report security incidents. Security personnel monitor the mailboxes regularly and assign the various e-mails to specific security officers, depending on the subject matter. Security incidents can also be reported to the DSO in person, by telephone or by e-mail.

Six security incidents were recorded in the INFC security incident log between January 2017 and December 2018: two suspicious e-mails; a lost boardroom key; a lost bag with potential secret documents; a missing activity log[10]; and personal information shared on an unencrypted USB key. INFC does not have a system in place to ensure that all reported security incidents are recorded in the security incident log. A review of the two security mailboxes revealed that security incidents are often dealt with directly through an exchange of e-mails between the various stakeholders without anyone recording the incident in the incident log. Cases were noted where there are incomplete series of e-mails and no evidence available as to how the incident was resolved.

In addition, several potential security incidents were noted in INFC documents, but were not recorded as security incidents. Examples include:

[10] An activity log is a report in which all the recorded computer events are sequentially ordered and displayed, such as a record of entrances and exits of employees to INFC facilities.

- Security violations were issued during security sweeps for not adequately protecting classified documents;
- An e-mail to Security Services reported a lost laptop;
- An encrypted USB key was reported lost;
- IT inventory records revealed that 21 encrypted USB keys, 4 laptops and 3 tablets have an unknown location and owner; and
- In July 2018, the Government of Canada – Computer Incident Response Team (GC-CIRT) notified INFC that suspicious files and/or network activity was detected on one of the INFC workstations. An infection was confirmed by INFC and the problem was resolved but not recorded as a security incident.

INFC receives weekly technical reports from the Canadian Centre for Cyber Security. The reports provide highlights of the incidents that affect Government of Canada departments. The INFC IT Security Coordinator reviews the weekly reports to identify incidents that could apply to INFC, but no record of the review is kept.

In conclusion, the process to manage security incidents at INFC needs improvement. At the moment, there is no assurance that all security incidents are properly identified, recorded, investigated, resolved and reported. It is important to record all security incidents through the appropriate channels to ensure that INFC has an accurate picture of the number and type of incidents. This measure will help INFC establish the overall departmental threat level and react correspondingly.

Recommendation #5:

It is recommended that the ADM Corporate Services, in consultation with the DSO, implement a process to adequately identify, record, investigate, resolve and report all security incidents.

Inventory controls

Criterion: There are adequate controls in place to prevent loss, damage, theft or compromise of the organization's physical, information and IT assets.

The audit focused on portable media devices such laptops, tablets, encrypted USB keys, and information assets. The controls over office furniture such as chairs and desks were not reviewed.

Security of IT assets

The 2007 INFC Department Security Policy requires that INFC establish and maintain an IT asset inventory. The INFC *Asset management Policy* states that: "*an IT asset inventory should be maintained to capture inventory details of all IT assets and track them throughout their lifecycle. Attractive items should be monitored particularly carefully on a regular basis to prevent loss, theft and abuse*". In its March 2019 - *Baseline Cyber Security Controls*, the Canadian Centre for Cyber Security recommends that strong asset controls be maintained

for all storage devices, including portable media devices, and requires the use of encryption on all of these devices.

All portable storage devices in use at INFC, including laptops, tablets and encrypted USB keys, have the data encrypted on them. In addition, all IT assets have an INFC asset tag and/or can be identified as belonging to INFC by the electronic serial number (e.g. encrypted USB keys). As part of the onboarding process, staff are briefed on how to protect the IT assets assigned to them and are referred to several security guidelines on the INFRAnet, including the *Policy on Acceptable Network and Device Use* and a *Publication on the Secure Use of Portable Data Storage Devices within the Government of Canada*.

INFC maintains a complete list of IT inventory items. As of February 11, 2019, there were 9,112 items in the INFC IT inventory. Items in the IT inventory listing included 1,736 computer monitors[11], 1,580 cell phones[12], 689 tablets, 490 laptops and 340 encrypted USB keys. In February 2019, a new software (Cherwell) was implemented to replace the existing software (BassetPro). However, all inventory records were transferred to the new system without being cleansed or validated. The current inventory records do not provide the value of each item or indicate which items are considered attractive.

INFC has not conducted a physical review of its inventory of IT assets for several years. As a result, the current inventory records contain a number of inaccuracies and it is difficult to assess how many items could have been lost, misplaced or stolen. For example, there are 119 items in the IT inventory with an unknown owner and location.

Security of information assets

In accordance with the TBS *Operational Security Standard for the Identification and Categorization of Assets*, departments must determine the criticality and sensitivity of their information with regard to confidentiality, integrity, availability and value. The INFC DSP requires that the Information Management manager, in collaboration with the DSO and IT Security coordinator, establish standards and procedures as they relate to IM security; and ensure the application of safeguards as they apply to information security – specifically in classifying and designating information; assessing threats and risks; and evaluating proposed safeguards for IM.

At the time of the audit, the majority of INFC's electronic records were stored in shared drives and Outlook mailboxes. INFC was in the process of implementing GCdocs (a Government of Canada system for saving, managing and sharing electronic information) to replace shared drives and to be compliant with the TBS *Directive on Recordkeeping*. INFC does not know the exact percentage of classified paper and electronic records, but given the business of INFC, it is estimated that there is a relatively limited amount of information that is sensitive and, therefore merits additional protection.

[11] Many INFC staff have dual monitors; quiet rooms, storage & dispositions make up the rest
[12] 496 are active and the rest are in storage. Of those, 850 BlackBerrys are to be disposed of and 234 cell phones are available to be deployed for digital briefcase)

INFC shared drives provide multiple information sharing platforms based on access and business processes. They are hosted and managed by SSC and are approved to handle classified information not exceeding Protected A without additional safeguards, such as encryption, and designed to reduce the residual risk for the department to an acceptable level. The audit found that information exceeding the approved security level was stored without additional protection in most of the shared drives that were examined, such as Cabinet documents classified "SECRET" (defined as those for which the unauthorized release could cause serious injury to the national interest - Annex D)[13]. The audit team did not attempt to determine if the documents had been under- or over- classified.

While most positions at INFC are classified as "SECRET", at the time of the audit about 115 positions were classified as "RELIABILITY". Restricting information access to staff security clearance is a fundamental element of the TB PGS, however the audit found that some staff had access to electronic information exceeding their security clearance. For example, the G:\Drive is accessible to all staff and 19 documents classified as "SECRET" were found there without additional safeguards.

The audit team did not attempt to determine if the positions were classified properly according to the nature of the work. However, the department is aware of the risk that some positions are misclassified. Security Services and Human Resources are currently using a tool to identify the security clearance requirement of new positions and required level of access to documents e.g. protected or classified. A plan will be developed to address existing positions.

Interviews with senior departmental staff revealed that the problems with the INFC shared drives are well known. While the implementation of GCdocs will address many of the issues for the Department, shared drives will continue to exist for a while as this takes place across the Department. It must be noted that GCdocs can handle only up to "Protected B" information.

In conclusion, opportunities exist to strengthen controls for the adequate protection of IT and information assets. Inventory controls for IT assets need to be improved and inventory records updated.

Recommendation #6:

It is recommended that the ADM Corporate Services, in consultation with the DSO:

- *Conduct a clean-up of the asset inventory records.*
- *Develop a risk-based asset control framework for safeguarding attractive IT assets.*
- *Implement compensatory controls such as monitoring how and where documents are saved, and increase awareness training for INFC employees to mitigate the risks of not appropriately managing classified documents.*
- *As part of the implementation of GCdocs, ensure that additional controls are implemented for any documents that exceed Protected B.*

[13] Source: INFC Guidelines on Handling Classified and Protected Information – 2016

Security in system development

Criterion: There are adequate security controls in place in the IT system development process to prevent IT systems being implemented without adequate security safeguards.

The TB PGS mandates that all IT systems must be security assessed and authorized (by completing the SA&A) prior to operation. INFC has a Project Management Framework (PMF) in place that consists of three project management phases with one or more stage gates that must be passed before the project can move to the next stage and/or phase. Security in system development is reviewed during the planning stage gate and the project execution stage gate.

There are a number of security requirements that need to be met before a system is allowed to be in production. During the planning phase, a System Profile Description (SPD) including a Security Plan (SP), a Statement of Sensitivity (SoS) and a Concept of Operations are prepared and approved. Prior to implementation, an evaluation of security controls is performed and includes the review of the Security Requirements Traceability Matrix (SRTM), a Privacy Impact Assessment (PIA) and a VA. The IT Security Coordinator manages the security assessment process and prepares the SA&A report that recommends either full authority, interim authority or no authority to operate.

During the audit, the two major IT projects listed in the INFC Investment Plan for 2018-19 to 2022-23 were reviewed. The Infrastructure Recipient Information System (IRIS), with a total cost of $3.6M, was implemented in 2018 and the GCdocs project, a Government of Canada system for saving, managing and sharing electronic information, is currently being implemented by INFC, with a total estimated cost of $2.15 million.

[redacted].[14]

GCdocs is the standard Enterprise Document and Record Management System for the Government of Canada. This tool will help INFC to meet its obligations in relation to information life cycle management and replace the existing desktop-based information technology tools and the use of shared network drives for information management. The

[14] Please note the audit has been processed in accordance with the *Access to Information Act* and certain information has been withheld from disclosure in accordance with exemptions in the **Act**

GCdocs business case was approved in January 2018. The system went into production in October 2018 and is being deployed throughout the organization during 2019-20.

[redacted]

[redacted].[15]

In conclusion, INFC has a Project Management Framework and SA&A process in place that is in compliance with the TB PGS and other policy instruments. Although not all older systems have current security certifications, the security in system development is functioning adequately for the new systems.

Physical security controls

Criterion: There are adequate physical security controls in place in the areas listed below to protect and safeguard information and assets:

- Identification and categorization of physical assets;
- Personnel security screening;
- Identification badges;
- Zoning; and,
- Storage, disposal and destruction of IT media.

The 2013 TBS *Operational Security Standard on Physical Security* contains both requirements and recommended safeguards for physical security. The 2014 TBS *Standard on Security Screening* covers the practices to provide reasonable assurance that individuals can be trusted to safeguard government information, assets and facilities, and to reliably fulfil their duties. Although not recent, these standards still reflect sound security practices.

[15] Please note the audit has been processed in accordance with the *Access to Information Act* and certain information has been withheld from disclosure in accordance with exemptions in the **Act**

INFC conducted TRAs using the Government of Canada's Harmonized Threat and Risk Assessment methodology for its four locations in 2017-18. The TRAs uncovered several areas of security concern and included a list of recommendations. For example, the 180 Kent TRA recommended that CCVE cameras should be added to the elevator foyer on each INFC floor to discourage potential tailgaters and support the identification of individuals accessing the floors. INFC included a summary of the TRAs findings in the DSP. At the time of the audit, INFC had already addressed a number of the TRAs' recommendations, had activities planned to address other areas of concern and in some cases, accepted the risk associated with certain vulnerabilities. The audit team reviewed the TRA reports and, for the most part, relied on the results of the TRAs. In addition, the audit team observed that the physical controls described in the TRAs, such as staff wearing identification badges, were, in fact, working during the period under examination.

INFC is responsible to ensure that all individuals who will have access to government information and assets are security screened at the appropriate level before the commencement of their duties. Only cleared personnel can have access to INFC workplaces and information systems. The personnel security screening process is key to determining which physical and information accesses a person will be granted. There are four different types of security clearance: Reliability, Confidential, Secret and Top Secret. At INFC, there is a well-defined process to ensure all staff and contractors have the required security clearance. Each INFC position has a pre-determined security clearance level that must be met by the incumbent. Consultant contracts stipulate the security clearance level required. The personnel security screening process was working well during the period under review.

In addition, INFC Security management identified a risk in that there is only one person responsible for security screening, with limited backup available. Given that INFC is currently both increasing in size and continuing to deal with turnover, the organization may want to take steps to further mitigate this risk, given that all new personnel requests must be handled by this function.

For the disposal, cleansing and/or destruction of electronic storage media, INFC follows the guidance of the Communications Security Establishment (CSE) in ITSG-06 *Clearing and Declassifying Electronic Data Storage Devices* and the March 2019 CSC *Baseline Cyber Security Controls for Small and Medium Organizations*. INFC uses the data sanitization methods recommended by CSE before the disposal or destruction of IT media.

For the most part, IT media at INFC consists of cell phones, tablets, laptops and encrypted USB keys. All of these media devices are required to have the data encrypted on them. Cell phones are wiped and returned to SSC after the contract expires, encrypted USB keys are erased to be re-used or physically destroyed, and tablets and laptops are either sent to Crown assets or to a school program after being wiped.

In conclusion, there are adequate physical controls in place, for the identification of physical assets, personnel security screening, identification badges, zoning and management of IT media.

4.3 Business Continuity Planning

Sub-objective: To determine whether the Department has established a Business Continuity Planning (BCP) Program that supports the continued availability of its critical and essential services and related assets.

Criterion: Business continuity plans have been developed based on results of the business impact analysis, have been appropriately approved, and are regularly tested.

Business Continuity Plan (BCP)

A BCP is a proactive planning process that ensures critical services and products are delivered during a disruption. These services and products are those that must be delivered to ensure survival, avoid causing injury, and meet legal or other obligations of an organization. Based on the 2009 TB PGS, the 2008 INFC *Business Continuity Planning Program Policy*, and the 2004 TBS *BCP Program Standard*, the continued delivery of government services must be assured through baseline security requirements, business continuity planning – including IM and IT continuity planning – and continuous risk management. BCPs should be developed based on the results of a Business Impact Analysis (BIA), appropriately approved, and regularly tested.

INFC has developed a BCP that applies to the recovery of INFC business services at each of its locations. It is important to note that the BIA identified no critical business functions or mission critical IT systems at INFC.

INFC refreshed its BCP in 2018. The process included interviews with subject matter experts to prepare the BIA, establishing a Business Continuity Response Team (BCRT), updating the BCP and performing two tabletop exercises. In addition, even though the BCP was not activated following the tornadoes in the National Capital Region in September 2018, it was updated following a post-mortem of that event. The BCP was presented to IMC and DMC before being approved by the DSO in November 2018. The BCRT met regularly in 2018 and ensured that information in the BCP, such as contact names and information, was kept current.

All parts of the BCP Program tested were up-to-date, in compliance with TB and INFC policies and standards and had been tested. The BCP contains the following components:

- Governance structure;
- Assessment of the situation;
- Scenarios and response strategies;
- Activation procedures;
- Recovery processes; and,
- Return-to-normal operations.

IT continuity planning

It is expected that Recovery Time Objectives[16] (RTOs) have been established for all IT systems and a Disaster Recovery Plan (DRP) aligned with the BCP has been prepared and tested.

While INFC has no mission critical IT systems, many programs depend on IT systems to enable their business processes. INFC has established RTOs for each IT system as part of the BIA process, but they reflect the recovery expectations of the system owner, rather than the maximum tolerable length of time that the IT system can be down in order to avoid unacceptable impacts on dependent business processes. For example, eight of the 18 IT systems in the BCP have an RTO of 24 hours or less, which is commonly reserved for mission critical applications as it requires a fully redundant system to be able to comply with the requirement.

INFC has not determined the associated costs to meet the established RTOs and has not included them in the Service Level Agreement (SLA) with SSC. In addition, INFC received no assurance from SSC that the RTOs can be met or whether they are regularly tested. In reality, SSC will recover INFC IT systems on a best effort basis and the RTO table will serve to prioritize the order of recovery.

In conclusion, INFC has a comprehensive BCP Program in place including a BIA and a BCP. The BCP is up-to-date and was tested twice in 2018. Given that INFC does not have any mission critical applications, the IT continuity part of the BCP should be reviewed to reflect more realistic RTOs for IT systems. Unrealistic RTOs may leave the system owners and management with the impression that there are systems in place to meet those targets in the event of a disruption or a disaster when it is not the case.

[16] **Recovery Time Objective (RTO)** is defined as the maximum tolerable length of time that a computer system, network, or application can be down after a failure or disaster occurs and defines the duration of time within which the IT system must be restored after a disaster (or disruption) in order to avoid unacceptable impacts on dependent business processes.

5. Conclusion and Recommendations

Moderate improvements are required for INFC to have a well-defined and fully effective departmental security program in compliance with the TB PGS and other relevant policies, directives and standards. The most important challenge faced by INFC is the cultural change necessary to move to a more security-conscious organization, and to implement the new TB PGS and other relevant departmental policies, directives and standards going forward.

A complete list of recommendations can be found in Section 7: Management Response and Action Plan.

6. Statement of Conformance

In my professional judgement as Chief Audit and Evaluation Executive, the audit conforms to the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing and the Government of Canada's Policy on Internal Audit, as supported by the results of the Quality Assurance and Improvement Program.

_____

Isabelle Trépanier
Chief Audit and Evaluation Executive
Audit and Evaluation Branch, Infrastructure Canada

7. Management Response and Action Plan

INFC Security Services continues to look for ways to improve the general security posture of the organization within its operating context. This will be done by increasing security awareness and applying approved risk mitigations through the defined governance process.

#	Recommendations	Priority Rating	Management Response and Action Plan	OPI and Due Date
1	*It is recommended that the ADM, Corporate Services, in consultation with the DSO develop and implement a process to ensure that all key security risks are identified, assessed and managed. This includes assessing performance against the Communications Security Establishment's Top 10 security actions for which the department is responsible, to ensure alignment with best practices to protect INFC's networks and information.*	High risk exposure	A central risk register will be developed, implemented Annual review of risk register Annual assessment of compliance against CSE Top 10 IT security actions	DSO Nov 29, 2019 March 31, 2020 March 31, 2020 (Sept 30 for subsequent years in line with Cyber Security Month in October)
2	*It is recommended that the ADM, Corporate Services, in consultation with the Director, Applications Services, conduct periodic reviews of user accesses to INFC's IT systems with a focus on users with privileged and administrative access rights.*	Medium risk exposure	A yearly review of accounts will be implemented on INFC's IT systems focussing on privileged and administrative access rights.	*Director, Applications Services* September 30, 2019
3	*It is recommended that the ADM, Corporate Services, in consultation with the DSO, review and revise awareness initiatives to ensure key risk areas,*	Medium risk exposure	Awareness initiatives revised & reviewed twice a year by Departmental security governance.	Nov 29, 2019 (Sept 30 and March 31st in

#	Recommendations	Priority Rating	Management Response and Action Plan	OPI and Due Date
	including compliance with the clean desk policy, are adequately communicated to INFC employees and tested for effectiveness.			subsequent years)
4	*It is recommended that the ADM, Corporate Services, in consultation with the DSO, establish and periodically report to senior management and the DM on metrics related to the security culture at INFC, such as statistics on infractions found during security sweeps.*	Medium risk exposure	Security reports will be delivered twice a year and reviewed by the Departmental security governance.	DSO Nov 29, 2019 (Sept 30 and March 31 in subsequent years)
5	*It is recommended that the ADM Corporate Services, in consultation with the DSO, implement a process to adequately identify, record, investigate, resolve and report all security incidents.*	High risk exposure	A tracking process will be Implemented to identify, record security incidents and associated investigations & resolutions regardless of severity.	DSO March 31, 2020.
6	*It is recommended that the ADM Corporate Services, in consultation with the DSO:* • *Conduct a clean-up of the inventory records.* • *Develop a risk-based asset control framework for safeguarding attractive IT assets.*	Low risk exposure	• An updated asset IT inventory will be completed. • The risks associated with asset control of electronic storage devices and "attractive" IT assets are captured as part of the risk register, which is to be reviewed annually.	DSO Mar 31, 2020 Nov. 29, 2019

#	Recommendations	Priority Rating	Management Response and Action Plan	OPI and Due Date
	• *Implement compensatory controls such as monitoring how and where documents are saved, and increase awareness training for INFC employees to mitigate the risks of not appropriately managing classified documents.* • *As part of the implementation of GCdocs, ensure that additional controls are implemented for any documents that exceed Protected B*		• Positional Analysis Tool is being used for new positions to identify the security clearance requirement of the position and level of access to documents e.g. Protected or classified. • Mitigation measures developed for "repeat offenders" as per the Clean Desk policy. • GCdocs security will be configured to restrict access to documents based on roles; • A report will be prepared twice a year, to highlight documents above protected B in GCdocs. • The risks associated with Secret documents will be captured as part of the risk register, which is to be reviewed annually.	April 4, 2019 March 31, 2020 March 31, 2020 March 31, 2020 Nov. 29, 2019

Annex A: Audit objective, sub-objectives and criteria

Audit Sub-Objectives	Audit Criteria
1: Governance: To determine whether there is an effective governance structure in place that supports transparent planning and decision-making related to departmental security.	1.1 Complete, approved and up-to-date policies and directives exist for departmental security.
	1.2 Roles and responsibilities for managing the departmental security program have been established, communicated and assumed.
	1.3 A communication strategy is in place to ensure that employees are informed of their security roles and responsibilities.
	1.4 Security risks are systematically identified, documented, assessed and mitigated.
2: Security controls: To determine whether there are sufficient and adequate departmental security controls in place to support security for individuals, facilities, physical assets, information management, and IT systems.	2.1 Access controls are implemented and reviewed periodically to protect facilities and IT systems.
	2.2 A security awareness program is in place to guide individuals and ensure that they understand and comply with their security responsibilities and do not unintentionally compromise security.
	2.3 There is an effective process to identify, monitor, analyze, assess and report security incidents in a timely manner.
	2.4 There are adequate controls in place to prevent loss, damage, theft or compromise of the organization's physical, information, and IT assets.
	2.5 There are adequate security controls in the IT system development process to prevent IT systems being implemented without adequate security safeguards.
	2.6 There are adequate physical security controls in the areas listed below to protect and safeguard information and assets: • Identification and categorization of physical assets; • Personnel security screening; • Identification badges; • Zoning; and • Storage, disposal and destruction of IT media.

Audit Sub-Objectives	Audit Criteria
3: Business Continuity Planning: To determine whether the Department has established a Business Continuity Planning (BCP) Program that supports the continued availability of services and their associated assets and resources.	3.1 Business continuity plans have been developed based on results of the business impact analysis, have been appropriately approved, and are regularly tested.

Source: The audit objectives and criteria were developed based largely on TB *Policy on Government Security*, TB *Policy on Information Management*, TB *Management of IT Security Standard*, TB *Standard on Physical Security*, INFC *Departmental Security Policy*, COBIT 5, and ISO 27001.

Annex B: INFC – Security RACI Chart

	INFC - SECURITY RACI Chart	Functions																	
	ACTIVITIES	DMC	IMC	Deputy Minister	ADM Corporate Services	Chief Information Officer	Departmental Security Officer	Manager Security	IT Security Coordinator	Manager Information Management	Manager Network Services	Director Application Services	Business Process Owner	TBS - CIOB	Shared Sevices Canada				
1	Develop and maintain GoC security policies and standards	I	I	I	C	I	C	I	I	I	I	I	I	A/R					
2	Develop and maintain INFC security policies and standards	I	I	I	C	C	A	R	C	C	C	C	I						
3	Create and maintain the Departmental Security Plan	I	I	A	C	C	R	C	C	C	I	I	I	I					
4	Maintain and monitor a security risk register					I	A	R (1)	R (2)	C	C	C							
5	Establish, maintain and monitor a security data classification scheme				I	A	C	C	C	R									
6	Manage inventory physical assets						A	R											
7	Manage inventory information assets					A				R									
8	Manage inventory IT assets					A					R								
9	Assure adequate security controls are included in project development.					C	A	R (1)	R (2)			C/R	C						
10	Track and manage applications security requirements (SA&A Process)						A	C	R			C/R	C						
11	Develop, deliver, monitor security awareness activities	I	I	I	I	C	A	R	C	C	C	C	I						
12	Establish and periodically review access rights and privileges (Physical)						A	R											
13	Establish and periodically review access rights and privileges (IT)					C	C		C		R	A	C		R (3)				
14	Define and monitor security incidents						A	R (1)	R (2)										
15	Conduct regular vulnerability assessment				I	I	A	R (1)	R (2)				I						
16	Develop, maintain and test Business Continuity Plan (BCP)		I		I	I	A	R					C	I	C				

R: Responsible: Person who performs an activity or does the work.	(1): For Corporate Security
A: Accountable: Person who is accountable and has Yes/No/Veto.	(2): For IT Security
C: Consulted: Person that needs to feedback and contribute to the activity	(3): For IT infrastructure
I: Informed: Person that needs to know of the decision or action.	

Annex C: Scorecard

Audit of Departmental Security at Infrastructure Canada			
Criterion	**Rating**	**Conclusion**	**Rec. no.**
Governance			
1.1 Policies, Directives and Guidelines		Security policies for INFC are in place but need to be updated and approved. INFC is well on its way to streamline and update its security directives and guidelines to align with the TB policy suite reset. However, INFC needs to establish a timeline for completing this now that the TB policy has been approved.	
1.2 Roles and responsibilities		Roles and responsibilities for the INFC security program are well defined and assumed.	
1.3 Communication		Widespread security communication tools are in place and easily accessible to staff (e.g. onboarding process, security posters, computer pop-ups and security pamphlets.)	
1.4 Risk management		Although there is an alignment between the Corporate Risk Profile and the associated security risks, the management of security risks needs to be improved to ensure all important ones are identified, recorded, investigated, resolved and reported.	1
Security Controls			
2.1 Access controls	IT Physical	Access controls to INFC facilities are well defined and implemented. Improvements are required for IT controls, especially for the management of privileged accounts.	2
2.2 Security awareness		A comprehensive and up-to-date security awareness program is in place. However, as of March 31st, about 33% of staff had not taken the mandatory security awareness course and recent security sweeps highlighted a lack of compliance by staff.	3
2.3 Incident Management		The system to manage security incidents needs to be improved. There is no effective process in place to ensure all security incidents are properly identified, dealt with in a timely manner and adequately reported to the DSO.	4
2.4 Inventory Controls		The new inventory system at INFC contains a significant amount of incorrect information. There is information with a security rating that exceeds that of the INFC shared drives it is kept in. In addition, staff have access to information requiring a higher security clearance.	5
2.5 Security in system development		The two IT projects recently implemented complied with the INFC Project Management Framework and the security requirements were met.	
2.6 Physical security controls		There are adequate physical controls in place for the identification of physical assets, personnel security screening, identification badges, zoning and	

		management of IT media. Security in the P3 storage room could be improved.	
Business Continuity Planning			
3.1 Business Continuity Plan (BCP)	IT Facilities	There is an up-to-date, approved and tested Business Continuity Program in place. Moderate improvements are needed to ensure Recovery Time Objectives for IT system are realistic and can be met in case of a disruption or disaster.	

Criterion met. Most systems and practices in place. No or minor improvements needed.	Criterion partially met. Many systems and practices in place. Needs moderate improvements.	Criterion not met. Some systems and practices in place. Significant improvements required.

Annex D: Document classification

Classification	Risk	Examples
Protected A	Unauthorized release could cause injury to an individual, organization or government. Loss of privacy or embarrassment	• Contracts and tenders • Date of birth • Home address and telephone number • Personnel Record Identifier (PRI) • Letters of offer
Protected B	Unauthorized release could cause serious injury to an individual, organization or government. Prejudicial treatment, loss of reputation or competitive edge.	• Treasury Board papers • Social Insurance Number (SIN) • Solicitor-client privilege • Contract negotiations • Risk assessments • Government decision-making documents • Criminal, medical, psychiatric or psychological records
Protected C	Unauthorized release could cause extremely serious injury to an individual, organization or government. Significant financial loss or loss of life.	• Records identifying persons deliberately spreading a life-threatening infectious disease • Information that could cause bankruptcy • Testimony against another individual
Confidential	Unauthorized release could cause injury to national interest	• Federal-Provincial Affairs • International affairs and defence • Private views of officials not intended for disclosure • Premature disclosure would be detrimental to government plans and intentions
Secret	Unauthorized release could cause serious injury to national interest	• Cabinet documents • Vital law enforcement • Plans for the defence of areas and installations • Particulars of federal budget before its official release

Source: INFC *Guidelines on Handling Classified and Protected Information* - 2016

Annex E: INFC Application Portfolio

	Acronym	Application Name
1	TeamMate	Audit software to manage working papers electronically
2	PIMS	Program Information Management System
3	LEXICON	Lexicon
4	COGNOSBI	Integrated business intelligence
5	WebCIMS	Tool to track correspondence within the department
6	LaserFiche	Tool used to manage ATIP requests
7	Quotes	Quotes software
8	PBMS	Tool to help manage finances and contracts among fund centers
9	JIRA	Workflow and issue tracking application
10	CA Bank	Bank software
11	TFS	Team Foundation Server
12	Central Collab	Central Collabaration tool to share large electronic files with external partners.
13	IRIS	Infrastructure Recipients Information System
14	IFRS	Application used by delegated managers/employees to assist in budget management, forecasting and reporting
15	ITSM	IT Service Management Tool
16	Keep	Platform to manage the security infrastructure
17	GCDocs	Electronic Document Management System
18	Skype	Videoconference tool

Annex F: Abbreviations

ADM	-	Assistant Deputy Minister
BCP	-	Business Continuity Plan
BCRT	-	Business Continuity Response Team
BIA	-	Business Impact Analysis
CCVE	-	Closed Circuit Video Equipment
CIO	-	Chief Information Officer
CRP	-	Corporate Risk Profile
CSEC	-	Communications Security Establishment Canada
DM	-	Deputy Minister
DMC	-	Departmental Management Committee
DSO	-	Departmental Security Officer
DSP	-	INFC Departmental Security Plan
GC-CIRT	-	Government of Canada – Computer Incident Response Team
GCdocs	-	Government of Canada system for saving, managing and sharing electronic information
IM	-	Information Management
IMC	-	Investment Management Committee
INFC	-	Infrastructure Canada
IRIS	-	Infrastructure Recipient Information System
IT	-	Information Technology
ITSG	-	Information Technology Security Guidance
PIA	-	Privacy Impact Assessment
PGS	-	TB Policy on Government Security
PMF	-	Project Management Framework
RACI	-	Responsible, Accountable, Consulted, Informed
RTO	-	Recovery Time Objective
SA&A	-	Security assessment & Authorization
SOS	-	Statement Of Sensitivity
SRTM	-	Security Requirements Traceability Matrix
SSC	-	Shared Services Canada
SLA	-	Service Level Agreement
TB	-	Treasury Board of Canada
TBS	-	Treasury Board of Canada Secretariat
TRA	-	Threat and Risk Assessment
USB	-	Universal Serial Bus
VA	-	Vulnerability Assessment