Audit of Physical Security Management

Corporate Internal Audit Division
Natural Sciences and Engineering Research Council of Canada
Social Sciences and Humanities Research Council

Approved by the President on March 18, 2015

Catalogue No.:CR22-50/2015E-PDF
ISBN 978-0-660-03876-6

TABLE OF CONTENTS

This is an abbreviated version of the audit report as the release of the information contained in the full version may represent a risk to the security of SSHRC and/or NSERC. The information is withheld pursuant to section 16(2)(c) of the *Access to Information Act*.

1 BACKGROUND

The Natural Sciences and Engineering Research Council (NSERC) and the Social Sciences and Humanities Research Council (SSHRC)[1] support scholarly endeavors in Canada's post-secondary institutions, and report to Parliament through the Minister of Industry. The Agencies share a Common Administrative Services Directorate (CASD) in which the Corporate Security function is housed. The Corporate Security team (CST) is comprised of two employees: the Departmental Security Officer (DSO) and Deputy DSO. The DSO reports through the Deputy Chief Information Officer (CIO), to the CIO, to the Vice President, CASD.

The Treasury Board Secretariat's (TBS) Policy on Government Security (PGS) defines physical security as, "the assurance that information, assets and services are protected against compromise and individuals are protected against workplace violence"[2] and Departments and Agencies are expected to implement a security program to achieve the following results:[3]

- Information, assets and services are safeguarded from compromise and employees are protected against workplace violence;
- Governance structures, mechanisms and resources are in place to ensure effective and efficient management of security at both a departmental and government-wide level;
- Security incidents are effectively managed and coordinated within departments and government-wide;
- Interoperability and information exchange are enabled through effective and consistent security and identity management practices; and
- Continuity of government operations and services is maintained in the presence of security incidents, disruptions or emergencies.

Organizations must ensure security management is collaborative, coordinated and monitored, and also establish a framework that brings together the various functions responsible for elements of security, [4] and ensure all employees, at every level of the organization, are aware of and understand their responsibilities.[5] The overall success of an organization's security management program is contingent on effective planning, communication, organization-wide collaboration and oversight.

2 AUDIT RATIONALE

As part of the risk-based internal audit planning process, the Corporate Internal Audit (CIA) Division identified the Corporate Security function as an area meriting examination. This audit was included in the 2014-17 Risk-Based Audit Plan (RBAP) because:

- The Agencies have never conducted an audit of physical security;
- The TBS Policy on Government Security states that all departments and agencies must review their compliance periodically;

[1] NSERC and SSHRC shall be referred to throughout the reports as "the Agencies."
[2] Policy on Government Security, July 1, 2009, Section 3.1
[3] Policy on Government Security, July 1, 2009, Section 5.2
[4] Policy on Government Security, July 1, 2009, Section 3.3
[5] Directive on Departmental Security Management, July 1, 2009, Section 6.1.2

- The audit was identified in the NSERC-SSHRC 2014-17 Risk-based Audit Plan, which was approved by the Presidents in March 2014.

3 AUDIT OBJECTIVE AND SCOPE

Objective

The objective of the audit was to provide assurance that governance, internal controls and risk management practices related to physical security management are adequate and effective. The audit assessed the effectiveness and adequacy of the Agencies' security measures and management controls. The audit included an assessment of:

- Governance, roles and responsibilities of all parties involved;
- Physical security risk management processes and practices;
- Physical access to facilities, information, and assets; and,
- Employee awareness and compliance with policies and directives regarding physical security.

Scope

The scope of the audit included all NSERC-SSHRC headquarters facilities within Constitution Square in downtown Ottawa, and two of the five NSERC regional offices (RO). The scope included information and assets contained in those areas. Compliance to the Occupational Health and Safety Regulation was not included in the audit, nor were the security practices, controls and processes managed by the buildings in which NSERC-SSHRC are located.

4 AUDIT METHODOLOGY

The audit was carried out in accordance with the Institute of Internal Auditors (IIA) International Standards for the Professional Practice of Internal Auditing, as outlined in the International Professional Practices Framework (IPPF), and conforms to the *Internal Auditing Standards for the Government of Canada*, as supported by the results of the quality assurance and improvement program.

The planning phase of the audit included the conduct of preliminary interviews and the collection and review of documentation in order to understand the current state of security management within the Agencies. The audit program, including detailed audit criteria and procedures, was then designed based on the information gathered during planning, and focused on the objectives and the lines of enquiry defined above.

Subsequently, during the conduct phase of the audit, the audit team interviewed security practitioners, program managers and employees; observed the physical safeguards in different areas and locations; and, examined and assessed current security practices against best practices and guidance provided by TBS.

5 AUDIT TEAM

Chief Audit Executive:	Benjamin Cyr
Audit Principal:	Patricia Morrell

6 MANAGEMENT RESPONSE TO AUDIT RECOMMENDATIONS

ITEM	RECOMMENDATION	ACTION PLAN	TARGET DATE
1.	It is recommended that the Agencies ensure the Departmental Security Officer (DSO) coordinates the security program and the various functional areas responsible for security; and, formalize the DSO's role in the governance and oversight of the security program.	Agreed. Information and Innovation Solutions (IIS) will review and formalize the DSO role in the governance and oversight of the security program to ensure effective coordination of the security program including the functional areas for security.	September 2015
2.	It is recommended that the Agencies first update their environmental, risk and/or threat assessments to validate and/or identify key threats and risks to the Agencies' operational environment (including satellite offices); and, then develop, finalize and implement a Departmental Security Plan and other documents and plans such as the Business Continuity Plan and Disaster Recovery Plan.	Agreed. As part of the Departmental Security Plan (DSP), IIS is validating the threats and risks identified in previous Threat and risk assessments (TRAs) and conducting an environmental scan to further define the Agencies threats and risks in the current security environment. The DSP has identified the completion of the TRAs for Regional Offices as a key security risk mitigation activity in FY2015-16. Recommendations from the DSP and TRAs will be leveraged to update Agencies key security documents, including the BCP and DRP.	DSP Completion: April 2015 Completion of Regional Office TRAs: March 2016
3.	It is recommended that the Agencies ensure personnel security clearances are performed in alignment with the requirements outlined in the Policy on Government Security, which not only outlines requirements for employees, but also for third parties who access facilities, assets, and information.	Agreed. IIS will present options to the Agencies' management committees to ensure that personnel security screening is performed in alignment with the Policy on Government Security (PGS) while continuing to meet the business requirements of the Agencies.	September 2015

4.	It is recommended that the Agencies conduct a formal threat risk assessment of all facilities (including regional offices) to ensure access controls and monitoring tools are deployed to areas based on level of risk or sensitivity needs.	Agreed. IIS will conduct a TRA in the physical environments (including the NSERC regional offices) to ensure physical security controls and measures are implemented according to the level of risk and security zoning requirements.	March 2016
5.	It is recommended that the Agencies review and operationalize the directives and processes for labeling, handling and protecting its data, paper records, and electronic records.	Agreed. IIS will review the existing information classification guidelines for security purposes and explore various implementation approaches to maximize outcome.	March 2016
6.	It is recommended that the Agencies ensure requirements for managing and protecting third party data and information are clearly defined in SLAs and MOUs with other organizations.	Agreed. IIS will develop a process and implement a procedure to ensure agreements with other organization (i.e. SLAs and MOUs) contain the security requirements for managing and protecting third party data and information.	March 2016
7.	It is recommended that the Agencies develop a clear asset management directive (including accountability, processes, procedures and guidelines) and implement a central or integrated system that allows proper management of assets through all phases of an asset's lifecycle (procurement, inventory, assignment, recovery, disposal, etc.).	Agreed. Finance and Awards Administration will develop an asset management process which will allow proper management of assets through all phases of an asset's lifecycle. Procedures developed as part of the asset management process will clearly define the roles and responsibilities to establish accountability, the types of assets subject to the policy and the means and frequency of tracking using the new centralized system.	March 2016

8.	It is recommended that the Agencies develop and implement a mandatory security awareness program that is aligned with the DSP (once finalized), and that addresses the Agencies' security requirements and risks linked to operations, facilities, assets and information.	Agreed. IIS will develop and implement a comprehensive mandatory security awareness program that is adapted to the Agencies' security requirements and level of risks.	September 2016

7 APPENDIX I – Audit criteria

Audit Criteria have been derived from the TBS Policy on Government Security (2009), Directive on Departmental Security Management (2009), and from the OCG's Core Management Controls (2011).

1. **Physical Security roles and responsibilities are clearly defined and performed by the appropriate employee; and information and/or issues are reported at the appropriate level.**
   - The governance structure supporting Physical Security Management is defined, clear and adhered to.
   - Roles and responsibilities of individuals responsible for Physical Security Management are defined, clear and cover all mandatory aspects.
   - Roles and responsibilities of committees and senior management related to Physical security is defined, documented and adhered to.
   - Physical Security information, incident reports, and/or assessment results are reported to / monitored by management or management committees for discussion and/or decision.

2. **Physical access to the Agencies' facilities, assets and information is limited to authorized individuals who have been security screened at the appropriate level and who have a need for access.**
   - Secure perimeters/zones have been identified and are appropriately enforced.
   - The Agencies limit access to assets to appropriate/approved individuals, and have controls in place to protect these assets.
   - The Agencies have an established information classification protocol to identify, label, and properly store sensitive and protected information.
   - Individuals who have access to the Agencies' classified information, assets, and secure areas are security-screened, and their access is linked to their security clearance level and needs.
   - The Agencies have established procedures, guidelines, and monitoring of security (information, assets, and physical space) to support sound physical security management at satellite offices, and in telework scenarios.
   - The Agencies' networks security level adequately protects information assets.

3. **Employees are aware of and comply with their respective roles and responsibilities with regard to physical security**
   - The Agencies' employees are aware of physical security requirements.
   - Physical Security roles and responsibilities for physical security are understood and thoroughly adhered to by Agency employees at all levels.
   - Physical security information is available and regularly communicated to all staff.
   - Adherence to Physical Security Requirements is monitored, and issues are corrected.

4. **Physical Security threat identification and risk management processes are in place, adequate, efficient and working as intended.**
   - The Agencies have defined and documented a Physical Security risk management process.
   - The risk management process is a continuous, and the monitoring for possible threats/risks occurs on an ongoing basis to ensure emerging risks are addressed.
   - Previously identified physical security risks/threats were shared with senior management, analyzed and appropriate actions were taken to address the risks.
   - The Agencies have approved documented internal security plans that are reviewed on a regular basis to ensure they are relevant and up-to-date.

8 APPENDIX II – Definitions

Variations of the following are definitions outlined in TBS Policies, Directives, Standards & Guides, as well as the Emergency Management Planning Guide, 2010-11, published by Public Safety Canada.

Environmental Scan: The process by which key external and internal factors and risks influencing an organization's policy and management agenda are identified.

Risk Assessment: The concept of risk is defined as a product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making.

Threat Assessment: The process of identifying or evaluating entities, actions, or occurrences, whether natural or man-made that have or indicate the potential to harm life, information, operations and/or property.

Threat Risk Assessment (TRA): Is a process for:

- Identifying assets and resources and assessing the level of risk to those assets and resources
- Evaluating threats, including the motivation, intent, capability of a threat agent and the opportunity, likelihood and consequence of threat acts that could place the delivery of critical services at risk.
- Examining and evaluating potential disruptions and events for the purpose of determining vulnerabilities and the implementation of countermeasures to reduce vulnerabilities.

Business Impact Assessment (BIA): The process of analyzing the degree to which a department is exposed to risks and impacts that could affect its ability to function or its ability to provide for the continuous delivery of critical services. The process consists of several steps, including: determining critical services and their priorities; determining minimum service levels and maximum allowable downtimes; mapping dependencies to critical services; assessing risks and existing recovery capabilities; and, formulating strategies for recovery.

Departmental Security Plan (DSP): A Departmental Security Plan should detail decisions for managing security risks and outline strategies, goals, objectives, priorities and timelines for improving departmental security and supporting its implementation.

Business Continuity Planning (BCP): An all-encompassing term that includes the development and timely execution of plans, measures, procedures and arrangements to ensure minimal or no interruption to the availability of critical services and assets. The BCP Program is composed of four key steps:

- The establishment of BCP program governance;
- The conduct of a BIA;
- The development of business continuity plans and arrangements; and,
- The maintenance of BCP program readiness.

Emergency Management Plan (EMP): The development and implementation of plans to manage emergencies concerning all-hazards, including all activities and risk management measures related to prevention and mitigation, preparedness, response and recovery.