Industry Canada Industrie Canada

Industry Canada
Audit and Evaluation Branch

Follow-up to the Audit of Security Function January 2000

January 2002

Canada

Follow-up to the
Audit of Security Function - January 2000

REPORT

Introduction

The preliminary phase of the security audit took place in January 2000. Since the recommendations of the report would prompt Security Services Division (SSD) to take several significant actions in the Department's locations, both in the National Capital Region and in the regions, the Internal Audit Branch decided against proceeding with an exhaustive audit. Instead, a follow-up, scheduled for 2002, was set out in the audit plan. An action plan was formulated by SSD in December 2000. The follow-up to the Audit of Security Function – January 2000 was conducted in January and February 2002. The follow-up enabled the auditor to report on the progress of the actions taken by managers to correct the deficiencies identified in the internal audit, to assess the scope of the corrective action taken by management, to determine the extent of implementation, and to obtain supporting documents.

The follow-up to the internal audit is considered an important part of the internal auditing process. It should be stated that senior management of audited organizations is essentially responsible for taking the corrective action required to act on the recommendations made by the auditors. It is important to bear in mind that a follow-up review does not constitute a second audit of the audited organization.

The follow-up was conducted using internal audit methods commonly used in the government of Canada, and is based on guidelines provided by Treasury Board and the Auditor General. To that end, the auditor interviewed several people, including the manager and employees of the Security Branch and a regional security coordinator. The auditor also carried out document analyses.

Background

The objective of the security audit was to evaluate the efficiency of Industry Canada's security function and to identify key aspects of this function which should be subject to a more exhaustive audit.

Specifically, the objectives of the audit were to:

- Evaluate the management framework used by SSD, including the efficiency of the departmental security policy and its level of compliance with Treasury Board's security policy; and
- Evaluate the effectiveness and efficiency of security function delivery within the Department.

The Audit Report recommendations centred on five main themes, namely:

- Security organization;
- Security administration;
- Physical security;
- Personnel security and contract management; and
- Emergency security and management.

The "information technology security" component, which is under the responsibility of the Chief Information Office, was excluded from this audit because of its distinct nature. However, the functional relationships between the informatics security officer and SSD were assessed.

Since November 2001, responsibility for SSD has come under the Trade and Operations Branch – Operations Sector. The Director of Security Services Division reports to the Deputy Director General, Operations and Corporate Services. As part of this reorganization, a business continuity planning unit was established. The alignment of the new unit's duties and those of Security Division is under way. The events of September 11 have resulted in a change in priorities and a heightened awareness of security within the Department.

Findings

Theme 1: Security organization

The January 2000 Audit Report recommendations focussed on a comprehensive assessment of the services provided on a cost-recovery basis to both internal and external clients, on formulating a security plan, and on updating policies. They have been implemented or are currently being developed. A certain number of activities, however, remain to be completed in order to update the policies.

In fact, in 2000, following the audit, SSD discontinued cost recovery from internal clients. Also, a study by the Management Consulting Centre on improving resource and cost management is under way to establish the actual costs of services provided to external clients.

SSD employees actively participated in Treasury Board Security Policy Review committees. A new security policy is now available (February 2002). Related departmental policies dated back several years, some of which were produced before 1993. Initial steps were taken toward updating them. Now that the new Government Security Policy is available, internal policies will be updated.

Nevertheless, a fair amount of work remains to be done.

Theme 2: Security administration

The recommendations dealt with putting in place a formal security awareness program that would include the regions, creating a new classification guide, and enhancing awareness among the regions to ensure that any type of violation, breach or incident is reported to the SSD. These recommendations were acted on. The Report also indicated the need to establish a priority list of buildings and to conduct a threat and risk assessment. This recommendation still remains an element of risk.

A formal security awareness program was implemented at Industry Canada. Awareness kits were prepared and sent to the regions along with presentations and notes. SSD hired additional staff to move ahead with the project. During visits to the regions, the use of the kits was encouraged and staff were told of the importance of completing incident reports. Impact analysis is critical in identifying security-related deficiencies.

The Department's information classification guide is completed and available to all employees via Intranet. A booklet was distributed to employees to raise awareness of the areas covered in the document classification guide. A review committee will be set up, which will also deal with declassification policies. Following the division reorganization, a proposal was put forward to restructure the Security Services Division Intranet site to facilitate access and updating.

SSD recognizes the importance of threat and risk assessment. An assessment of physical threats and risks was conducted at two priority sites (C. D. Howe and Portage I). A list has not yet been completed for other sites because of a lack of funds. Immediate security needs in the regions will be examined during business continuity planning preparations, which are under development. SSD included a proposal to ensure delivery and updating of this activity in the budget reviews that are in progress. A threat and risk assessment will identify the assets, people and services that must be protected, and will explain any threats and vulnerabilities. It will also justify the level of protection required, and propose recommendations to minimize risk. Threat and risk assessment preparation is one of the mandatory features of the Security Policy, and is an integral part of the management process of being aware of and making decisions regarding risks.

Theme 3: Physical Security

The recommendations called for the preparation of a guide to ensure that all elements would be taken into account in cases of new construction or renovation, silent hour sweeps and the establishment of a periodic review and control program of physical security measures. These recommendations have been acted on, and awareness efforts are under way.

An effective program is in place to ensure that all elements are considered for new construction and renovation projects in the National Capital Region. The program, however, is not yet in place

in the regions. The regional security coordinator is responsible for developing guidelines for 2002-03.

Silent hour security sweeps are conducted in National Capital Region offices. Regional coordinators are responsible for conducting these sweeps in their regions. This practice is not common to all regions. In the course of these sweeps, positive or negative notes are left for employees. Sometimes little reminders, like pens, are left behind to indicate that a sweep was made and to promote the Security Awareness Program.

Regular visits are made to the regions to ensure that security controls are in place. A guide is available for these audits and is used during these visits. A report is updated. It must be noted that the level of security has been increased department-wide since the events of September 11. For example, sometimes over 400 temporary passes are issued in a single day to control access to buildings.

Theme 4: Personnel security and contract management

The recommendations focussed on the need to ensure that security rating checks are completed before employees begin work and that regular security rating updates are conducted within the prescribed deadlines. These recommendations have been acted on. A certain number of security rating updates are pending. The SSD is working to remedy the situation.

It is incumbent on the manager to ensure that security investigations are completed before employees take up their duties. An awareness program is in place and has been quite successful. Since its implementation, there have been few incidents. Since security measures have been stepped up, violators have usually been detected when requesting office access passes or computer access.

Employee security rating data have been migrated to the PeopleSoft databank. Reports are produced on a regular basis. Several (200) files remain to be processed for everything to be up to date. SSD is working hard to complete them.

Theme 5: Emergency security and management

The audit revealed that necessary measures have been followed to protect sensitive information and assets, as well as employees, during any type of emergency. Procedures are available for both security staff and employees. Consequently, no follow-up has been done.

Conclusion

The auditors are of the opinion that it appears that Security Services Division has taken sufficient corrective measures to correct most of the deficiencies observed during the audit. Some weaknesses indicated in this follow-up report must be considered. Action will be required to improve the policies and finalize the preparation of threat and risk assessments throughout the department.