A case study audit report of veterans affairs' association

Environment, Air

Introduction

The Veterans Affairs (VA) is subject to the Government Security Policy (GSP) and must ensure compliance with the GSP and operational standards. The VA is responsible for the conduct of an audit to determine the efficiency and effectiveness of its security program. At the request of the VA, we conducted an audit of security to provide management of the VA with an objective assessment of it security program. Overall, we found that the VA met the requirements of the Government Security Policy (GSP) with respect to compliance, efficiency, and effectiveness. The audit provides an overview of the main security measures we observed. We also identified areas for improvement.

The department of Veterans Affairs' Investigation

A Case Study Audit Report

Generally, the VA has put in place a security program which complies with the GSP and operational standards. The roles and responsibilities of Security Management, Personnel Security, Physical Security, Information Technology Security as well as Contracting Management Security and Contingency Measures Security are clearly defined in the Security Management Structure.

The Departmental security officer (DSO) carries out his duties by coordinating, controlling and updating the security program on a regular basis. The VA has implemented adequate mechanisms to ensure the protection of sensitive information and assets. The sensitive information and

assets are classified, designated, declassified or disposed of, in compliance with the standards. Emergency and recovery plans are periodically developed, documented and revised, in compliance with the requirements.

Public Works and Secure Impact (PWSI) is currently responsible for security screening services which are conducted in compliance with the Security Policy and the Personnel Security Standards. Even though the original agreement between the two parties for this service is no longer valid. Moreover, certain roles and responsibilities between the two parties are not clearly established and defined in the agreement. Presently, the VA determines the security level related to the position requirements and requests the appropriate personnel screening. The PWSI acts as the administrative security officer by granting the level of security requested by the VA.

About the Audit

The Veterans Affairs (VA) is responsible for protecting sensitive data such as financial, medical, and personal Veteran and employee information under their authority. The information must be classified and designated considering the provisions for adequate exceptions of the Access to Information Act and the Privacy Act. The data appropriate to information technologies must be classified and specifically designated per their confidentiality, integrity, availability and value. Information and sensitive data must be protected per minimal standards, and related risk and threat assessment.

The VA is responsible for the implementation of the Security Policy within its institution and must conduct an internal audit on their compliance with the policy and their efficiency in implementing it at least every year. This audit is conducted within the framework of Treasury Board Secretariat's requirements in this respect.

Objectives

The objectives of the audit are to ensure the compliance of all sensitive information and goods with the Government Security Policy (GSP) and with the operational standards and the efficiency and effectiveness of the Security Program of the VA. More specifically, the objectives focused on: Security organization, Security Management, Physical Security and Personnel Security.

Scope of the Audit

The audit covers the following:

Security Organization: the structure of security management at the VA for the overall security program.

Security Management: the security program, the security education and training programs, the classification and designation of sensitive data, the measures of protection for sensitive information, the breaches and violations of security and other security-related incidents, the protection measures taken for external communications.

Physical Security: the location and layout of installations, the identification and the application of protection measures in the installations, the examination and control of physical security measures.

Personnel Security: the personnel security investigations, the authorization, refusal and revocation of security levels, the measures required at employees’ termination of employment.

Security and management of emergency cases: necessary actions are taken to protect sensitive information and assets and employees during all types of emergencies.

Security and management of contracting: security measurements are included with other requirements in contracts involving access to sensitive information.

Approach and Methodology

The audit methodologies are comprised of interviews, data gathering, information and report analyses, the study of files and the observation of practices.

Findings and Management Responses

Security Organization

Objective: To verify whether there is in place a security management structure meeting the Agency’s requirements for the overall security

program, specifically management security, physical security and personnel security.

VA has implemented a security management structure which meets the overall security program needs of the Agency. The security responsibilities are clearly defined, established and assigned to personnel whose positions include security responsibilities defined in the position description. Secure Impact, a tenant in the same building as VA, is responsible for the development and implementation of the physical security. For personnel security screening VA depends on the services of PW.

Area of Improvement

The audit has found that the agreement between the VA and PW for the delivery of personnel security screening services has expired. Furthermore, certain roles and responsibilities of PW as related to the security of the VA personnel were not clearly established in the expired agreement.

Management Response

The VA recognizes the importance of maintaining valid agreements with its service providers, especially when dealing with security issues. The VA also appreciates the necessity of having clear roles and responsibilities defined in the agreement and understood by all parties.

After being apprised of the above situation, the VA contacted PW to begin negotiation on a new agreement, which would clearly state roles and responsibilities of all parties.

The VA will also ensure that this agreement is revised periodically and that it is extended, based on operational requirements.

Security Management

Objective: To verify whether a good security program is an integral part of the VA’s overall program and meets the GSP requirements and operational standards.

The VA currently has a good security program in place which complies with the requirements of the GSP and operating standards. The responsibilities assigned to security personnel are fully carried out. Guides and procedures have been developed which are used as guidelines for those in charge of security.

Area of improvement

Develop a security policy or adapt the TBS security policy to meet the VA requirements.

Management Response

The VA will review current Government Security Policy and determine how and if it can be adapted to meet VA requirements. Should this not be feasible, the VA will develop its own internal security policy.

It should be noted that although the VA has no official internal policy which covers all aspects of security, it does have a policy on electronic mail, which

sets out standards for ensuring that established security levels are adhered to and that needed information is preserved.

Objective: To verify whether there are good security education and training programs.

The VA does not have in place a security education and training program.

Area of improvement

Provide training to employee with security responsibilities.

Management Response

The VA is fully supportive in providing training to its employees. Each year, a training plan is submitted by employees and approved by the Chairperson. The VA will ensure that those employees with specific security functions are made aware of and encouraged to take training necessary to meet current and upcoming security requirements.

Objective: To verify whether sensitive information is classified and designated in compliance with the GSP and operational standards, and whether the classifications and designations are unclassified or eliminated when the information is no longer, or less of a sensitive nature.

The VA has implemented a mechanism to ensure that goods of a sensitive nature are classified and designated in compliance with the GSP and operational standards; the same mechanism is also being used to declassify or dispose of the same goods.

Area of improvement

No recommended improvement

Objective: To verify whether protection measures are applied for sensitive information, as well as for employees, in compliance with the mandatory standards and with a risk management methodology.

The VA has implemented mechanisms to ensure the security of sensitive information. A process is in place to declassify sensitive information when it is no longer sensitive. The controls in place ensure authorized to receive such information.

Area of improvement

No recommended improvement

Objective: To verify whether breaches of security, security violations and other security-related incidents that may happen are the subject of an enquiry, that measures are taken to minimize the losses and that the necessary administrative or disciplinary measures are taken if warranted.

Breaches of security, security violations and other security-related incidents are reported to Secure Impact. Secure Impact is responsible to take the necessary administrative measures and to ensure follow-up.

A mechanism is in place and is used to report security breaches and to prepare reports.

Area of improvement

No recommended improvement

Objective: To verify whether the necessary protection measures are taken for the sensitive information communicated to or from official sources outside the department.

The VA follows procedures concerning sensitive information transmitted to official sources outside the department.

Area of improvement

No recommended improvement

Physical Security

Objective: To verify whether consideration was given to providing good siting to, as well as adequate retrofit of installations, to reduce or eliminate threats and risks to which the information, and the employees in those installations are exposed.

The VA uses the facilities along with other government departments. Secure Impact ensures the physical security, thus reducing or eliminating threats and risks. A physical security committee is established with a representative of the VA. In this regards, the physical security is adequate.

Area of improvement

No recommended improvement

Objective: To verify whether the required physical protection measures are applied in installations, so that sensitive information is well protected.

The current physical protection measures ensure that sensitive information is protected.

Area of improvement

No recommended improvement

Objective: To verify whether the physical security measures required are applied in the installations to ensure the protection and security of staff.

Implemented physical security measures in the VA facilities ensure employee protection and security.

Area of improvement

No recommended improvement

Objective: To verify whether the physical security measures are periodically reviewed and controlled.

Security measures are reviewed and controlled periodically.

Area of improvement

No recommended improvement

Personnel Security

Objective: To ensure that the personnel of the VA is subjected to a security check per the Government Security Policy (GSP) and the standard on Personnel Security

The audit found that security checks were conducted in compliance with the Government Security Policy (GSP) and the standards on Personnel Security. PW is responsible for the safe storing of personnel records and for the filling in and storing of security investigation forms requests.

Area of improvement

No recommended improvement

Objective: To verify whether the necessary levels of security are authorized, refused and revoked per the GSP and to the personnel security standard, and whether such measures are taken in a just and impartial way.

The VA has no record of refusals or revocations of levels of security. The VA recognizes its responsibilities in this matter.

Area of improvement

No recommended improvement

Objective: To verify that the necessary measures are taken to reduce or eliminate any risk for the sensitive information and goods as well as for the department’s essential systems at the termination of employment.

The audit found that the necessary measures are taken at the termination of employment.

Area of improvement

No recommended improvement

Security and Contracting Management

Objective: Ensure that security requirements are included with other requirements in contracts when they involve access to sensitive information.

The VA does not have mechanisms in place to check authorization to access facilities by the contracting parties.

Area of Improvement

Put in place a mechanism to check the authority to access the facilities by the contracting parties.

Management response

The VA is fully aware of its responsibility to ensure that only those individuals with proper authority are given access to its facilities. In some cases, authority to access VA facilities is given by another department, such as Secure Impact, but the VA is informed in advance. The VA will ensure that in those situations where another department gives access to its facilities, once the individuals show up, their name and authority will be verified with the other department.

Conclusion

The audit provides an overview of the main security measures observed, as well as, identifies areas for improvement. The audit methodologies are comprised of interviews, data gathering, information and report analyses, the study of files and the observation of practices. Finally, the audit covers security organization, security management, physical security, personnel security, security and management of emergency cases, and security and management of contracting.

Reference

http://andrei. clubcisco.
ro/cursuri/5master/sric-asr/cursuri/Readings/secaudit. pdf