Service | Innovation | Value

Audit of Departmental Security

Audit Report

Office of Audit and Evaluation
March 2015

Shared Services Canada
Services partagés Canada

Canada

TABLE OF CONTENTS

Executive Summary

What we examined

The objective of this audit was to determine whether Shared Services Canada (SSC) was implementing a security policy framework that was consistent with Treasury Board (TB) policies regarding security and whether Security Assessment and Authorization (SA&A) processes were in place and working as intended.

The scope of the audit included SSC's security policy framework and the SA&A process from April 1, 2012 to October 31, 2013.

Why it is important

Security of information, assets and services is essential to protect information against compromise and ensure that individuals are protected against workplace violence. TB established specific policies regarding departmental security management.

SSC was established on August 4, 2011, and its security function began in January 2012. This audit examined SSC's departmental security function.

What we found

We found that SSC developed a security policy framework that was consistent with most key government policies, although minor exceptions were noted, management has agreed to address once the revision of Management of Information Technology Security Standard is completed.

To comply with TB requirements to conduct risk management activities, SSC had a documented and approved Information Technology Security Risk Management Framework (ITS RMF) (the Framework) that prescribed the SA&A process. However, ownership of this document had not been determined.

Roles and responsibilities for the conduct of the SA&A had been defined in the ITS RMF as well as in the SSC SA&A Guide (the Guide). The Framework and Guide were available to SSC employees.

None of the corporate information technology applications implemented during the scope of the audit had completed the SA&A process. Project managers confirmed that they implemented applications without completing the SA&A as the process was considered to be overly time consuming to meet the implementation demands.

Project managers identified three key reasons for not completing the SA&A for the corporate application: unclear understanding of the process, the process not being included in projects' implementation calendars and the level of effort not being scalable to the associated risks of the applications.

Yves Genest
Chief Audit and Evaluation Executive

Background

1. The Treasury Board (TB) Directive on Departmental Security Management states that the management of security is an essential component of the effective management of a department and the government as a whole. This directive further states that departmental security activities must be centrally coordinated and systematically woven into day-to-day operations to ensure that individuals, information, assets and services are safeguarded, departments do not increase risks to other departments or the government as a whole, and critical services and operations continue in the event of an emergency.

2. Shared Services Canada (SSC) was established on August 4, 2011, to modernize how the federal government manages its information technology (IT) infrastructure in order to better support the delivery of programs and services to Canadians. The first step toward establishing a formal security function at SSC was taken in January 2012, with the appointment of a Chief Information and Security Officer (CISO), who was also the Departmental Security Officer, and a Director of Security. Prior to these appointments, there was no formal security structure for SSC.

3. Departmental Security, a division of the CISO, was responsible for the management and operation of the Department's Internal Security program. The division was comprised of three sections, each responsible for their respective functions: IT Security, Security Operations and Internal Security.

4. Departmental Security was responsible for designing measures to protect the security and integrity of SSC programs, information, assets, people and working environment. These measures related to:
    - Physical Security;
    - Security Issues and Investigations;
    - IT Security;
    - Security and Emergency Management Policies;
    - Security Awareness;
    - Emergency Management and Business Continuity;
    - Building Emergency Organization;
    - Fire Safety;
    - Personnel Security; and
    - Forms.

5. The internal audit team reviewed the policies and procedures prepared by security officials to ensure compliance with key government policies. Included in those policies was the Security Assessment and Authorization (SA&A) process, (formerly known as the Certification and Accreditation process) which was required to ensure that systems and applications were appropriately secured to meet levels of acceptable risk. The review of the SA&A process was conducted to determine if risks associated with using corporate IT systems to support business activities were being addressed at SSC.

Objective

6. The objective of this audit was to determine whether:
    - SSC was implementing a security policy framework that was consistent with TB policies regarding security; and
    - SA&A processes were in place and working as intended.

Scope

7. The scope of the audit included SSC's security policy framework and the SA&A process from April 1, 2012, to October 31, 2013.

8. This included all policies, guides, documents and data pertaining to departmental security at SSC in this timeframe. This did not include the security associated with services provided to partner departments and clients.

Methodology

9. During the conduct of the audit we:
    - Interviewed senior management, project managers and technical experts;
    - Reviewed TB, Government of Canada and SSC documents; and
    - Conducted SA&A process walkthroughs.

10. Field work for this audit was substantially completed by April 1, 2014.

Statement of Assurance

11. Sufficient and appropriate procedures were performed and evidence gathered to support the accuracy of the audit conclusion. The audit findings and conclusion were based on a comparison of the conditions that existed as of the date of the audit, against established criteria that were agreed upon with management. This engagement was conducted in accordance with the Internal Auditing Standards for the Government of Canada and the International Standards for the Professional Practice of Internal Auditing. A practice inspection has not been conducted.

Detailed Findings and Recommendations

Security Documents and Processes

12. We expected SSC to be compliant with government security policies and directives. We reviewed the SSC products designed to address TB requirements, such as the SSC Departmental Security Plan (DSP) and the draft Policy on Departmental Security (PDS). SSC was in compliance with key TB security requirements. Minor exceptions were noted pertaining to the TB Management of Information Technology Security Standard (MITS), and management has agreed to address these minor exceptions once the revision of MITS is completed.

13. Throughout the development of the DSP, internal and external consultations were conducted in order to ensure the validity of the information presented. The consultative process resulted in a list of the highest risks for SSC with a further risk analysis to assess the likelihood and impact of these security risks and how they could affect the achievement of SSC's strategic and business outcomes. This work resulted in an implementation plan that included the recommended controls to address the gap, resources required and estimated completion.

14. As required by the TB *Policy on Government Security*, SSC developed and approved a DSP which outlined security control objectives, deficiencies and their action plans, as well as roles and responsibilities pertaining to performance measurement and reporting. We found that SSC implemented most of the security controls set for completion by the end of fiscal year 2013–2014. Those controls, though not implemented at the time of the audit, were on-track for completion by their deadlines.

15. The Department had a documented and approved PDS. The PDS was the primary instrument for communicating security roles, responsibilities and accountabilities at SSC. While there was no requirement to communicate the PDS, management was planning to communicate the policy to employees.

16. We found that SSC developed policies and procedures that were consistent with requirements listed in most TB policies. Roles and responsibilities were defined within the policy framework with plans in place for communication to staff. There was monitoring and reporting on security controls with progress being made toward full and timely implementation. In addition there was regular interaction with Treasury Board of Canada Secretariat officials to ensure continued compliance with government security policies.

The SA&A Process

17. As part of the risk management activities required by the TB *Policy on Government Security*, we expected SSC to implement risk management activities regarding IT applications. We also expected SSC to conduct the SA&A process as corporate IT systems were implemented.

18. We found that SSC implemented a risk management framework as required by the TB Policy. The Information Technology Security Risk Management Framework (ITS RMF) was approved April 1, 2012, by the CISO and the Executive Director, Identity Management and Security. The ITS RMF was developed by SSC in collaboration with TB and the Communications Security Establishment Canada (CSEC) to implement the new continuous risk management framework as defined in CSEC's IT Security Guide-33. The previous Certification and Accreditation process was renamed the SA&A process. A guide developed by IT Security was shared with employees to be used in association with the ITS RMF.

19. We found the ownership of the SSC ITS RMF was unclear. Both the CISO, who had responsibility for corporate applications, and the Director General, Cyber and IT Security Transformation Program (DG CITS), who had responsibility for all non-corporate applications, indicated that they owned the Framework. Unclear ownership of the Framework could impact the communication, enforcement and application of the SA&A process. In addition, this could result in two different SA&A processes within SSC leading to additional confusion.

20. We identified 23 corporate IT applications that were implemented during the scope of this audit. These applications were required to have the SA&A conducted as stipulated in the TB *Policy on Government Security*. We found that none of these applications had completed the SA&A process.

21. We met with the six project managers responsible for the implementation of these 23 applications. The project managers identified three key reasons for not completing the SA&A for these applications: unclear understanding of the process, the SA&A process not being included in the projects' implementation calendars, and the level of effort not proportionate to the associated risks of the applications.

22. We found communication from senior management was limited regarding the requirements of the SA&A process. The first communication regarding the SA&A process was in September 2013, by the Manager of IT Security. Prior to this, only one of six project managers interviewed received information regarding the SA&A process at SSC. It was unclear to project managers what the expected process was at SSC, although some had prior experience with the SA&A process prior to joining SSC. Some stated that clear communication from more senior management would have supported the process being more consistently followed.

23. The SSC ITS RMF, along with the SA&A Guide, identified that the project managers were required to complete an SA&A as part of the projects' lifecycle. While SSC had a defined and implemented project governance framework, we found that the SA&A process was not integrated into the existing project management methodology. Early integration of SA&A into the project lifecycle, as part of the project management methodology, would improve the controls to ensure the SA&A process was completed.

24. During interviews, concerns were raised by project managers regarding the length of time and demand on resources to comply with the SA&A process. Urgency to implement corporate applications sometimes created pressure to circumvent the certification process. Many of those interviewed did not believe they could complete the required paperwork under such time constraints and, therefore, they would accept the risk of not completing the process. We found a lack of controls to ensure that applications were implemented with a completed SA&A.

25. Both senior management and project managers indicated that the SA&A process should be proportionate to the associated risks rather than an identical process for each application regardless of the risk. For example, an off-the-shelf application that is used in several other departments should not require the same level of scrutiny than a newly developed in house application. The SA&A process was not considered flexible. Many of the applications implemented in SSC during the scope of the audit were well known and commonly used corporate applications in government, such as Windows 7, PeopleSoft and SAP.

26. SSC had a documented and approved ITS RMF that prescribed the SA&A process. The roles and responsibilities for the conduct of the SA&A were defined in the SSC ITS RMF. The conduct of the SA&A process to corporate applications was limited and all applications were implemented without a completed SA&A. Failure to conduct the SA&A resulted in non-compliance with the SSC Framework. In addition, this meant that risk management activities required by the TB *Policy on Government Security* were not conducted. Therefore, we were unable to determine whether the IT security risks associated with each application were identified and mitigated.

Recommendation 1

The Senior Assistant Deputy Minister, Corporate Services, should clarify and communicate the ownership and roles and responsibilities pertaining to the Information Technology Security Risk Management Framework between the Chief Information and Security Officer and the Director General, Cyber and Information Technology Security Transformation Program.

Management response:

The Senior Assistant Deputy Minister, Corporate Services (SADM CS) agrees with this recommendation.

The CISO and the DG CITS, Transformation, Service Strategy and Design, frequently confer on matters related to security risk and security assessment.

Annex C of the SSC Policy on Departmental Security, published on May 21, 2014, contains the IT security roles and responsibilities of the three branches that have IT security responsibilities. In addition, a RACI matrix[i] is currently being developed.

Recommendation 2

The Senior Assistant Deputy Minister, Corporate Services, should develop and implement a communication plan, including the involvement of appropriate levels of management, to stakeholders involved in the implementation of corporate information technology systems.

Management response:

The SADM CS agrees with this recommendation.

[i] Responsible, Accountable, Consulted, Informed (RACI) matrix

It is important that project managers understand the security risks inherent to deploying applications and systems and that the Authorizer accepts or does not accept the assessed risk. The Authorizer is the Director General in CS responsible for managing the assessed corporate application or system.

Recommendation 3

The Senior Assistant Deputy Minister, Projects and Client Relationships, should integrate the Security Assessment and Authorization process for corporate applications into Shared Services Canada's project management methodology.

Management response:

The SADM Projects and Client Relationships (*PCR) agrees with this recommendation.*

The Project Management Centre of Excellence, PCR, has established a rigorous process for managing information technology projects. Adopting this methodology for corporate applications should ensure that SA&A processes are properly conducted for application development projects.

Recommendation 4

The Senior Assistant Deputy Minister, Corporate Services, should revise the Security Assessment and Authorization process to take into account the risk associated with the application being implemented.

Management response:

The SADM CS agrees with this recommendation.

The CISO is undertaking an Application Portfolio Management strategy to evaluate the end state list of SSC enterprise applications. This strategy will provide a list of applications that will require an SA&A process.

Recommendation 5

The Senior Assistant Deputy Minister, Corporate Services, should implement controls that ensure the Security Assessment and Authorization process is properly completed before the implementation of corporate applications.

Management response:

The SADM CS agrees with this recommendation.

Conclusion

27. The objective of this audit was to determine whether SSC was implementing a security policy framework that was consistent with TB security policies and that SA&A processes were in place and working as intended.

28. SSC developed a security policy framework that was consistent with most key government policies, although minor exceptions were noted. A DSP was established with defined roles and responsibilities, monitoring and reporting functions, and performance measurement features identified for further development. A PDS was developed and approved by the President of SSC. Communication to SSC employees was pending.

29. SSC had a documented and approved ITS RMF that prescribed the SA&A process. The ownership of this document had not been determined between the CISO and the DG CITS which had implications for accountability pertaining to enforcement.

30. We found that roles and responsibilities for the conduct of the SA&A had been defined in the SSC ITS RMF, as well as in the Guide. The Framework and Guide were available to SSC employees.

31. None of the corporate IT applications implemented during the scope of the audit had completed the SA&A process. We were able to identify only a few applications that had some of the documentation prepared. Project managers confirmed that they implemented applications without completing the SA&A as the process was considered to be overly time consuming to meet the implementation demands.

32. Those having responsibility for the SA&A process suggested that implementation activity supported by communication from the CISO would increase the usage of the process.

33. Consideration should be given to the scalability of the process and the resources required to complete the required documentation as well as controls to ensure completion of the SA&A prior to the implementation of a corporate application. Integrating the SA&A process into SSC’s project management methodology may increase compliance.

Management Response and Action Plans

Recommendation 1

The Senior Assistant Deputy Minister, Corporate Services should clarify and communicate the ownership and roles and responsibilities pertaining to the Information Technology Security Risk Management Framework between the Chief Information and Security Officer and the Director General, Cyber and Information Technology Security Transformation Program.

Management Action Plan	Position Responsible	Completion Date
Quarterly tri-lateral meetings will be scheduled with the Chief Information and Security Officer, the Director General, Cyber and Information Technology Security-Transformation, Service Strategy and Design and the Director General, Information Technology Security Operations. The Information Technology Security Risk Management Framework will be a standing item on the agenda. Expected results: There is clarity regarding the roles and responsibilities for IT security risk management.	Senior Assistant Deputy Minister, Corporate Services	September 30, 2014

Recommendation 2

The Senior Assistant Deputy Minister, Corporate Services should develop and implement a communication plan, including the involvement of appropriate levels of management, to stakeholders involved in the implementation of corporate information technology systems.

Management Action Plan	Position Responsible	Completion Date
The Chief Information and Security Officer will collaborate with Internal Communications to design the most effective and appropriate communications plan and to implement the plan quickly. Expected results: Awareness of the importance of information technology security risk management is raised as a result of this action plan and the action plan for recommendation 3.	Senior Assistant Deputy Minister, Corporate Services	March 31, 2015 and ongoing

Recommendation 3

The Senior Assistant Deputy Minister, Projects and Client Relationships should integrate the Security Assessment and Authorization process for corporate applications into Shared Services Canada's project management methodology.

Management Action Plan	Position Responsible	Completion Date
The Chief Information and Security Officer (CISO) will confer with the Project Management Centre of Excellence (PMCoE) to ensure that the Security Assessment and Authorization process is integrated into the SSC Project Management methodology for application development projects. The CISO, through continuing communications, will ensure that the PMCoE methodology is used for CISO application development projects. Expected results: Security risk management is included in the application development project life cycle.	Senior Assistant Deputy Minister, Projects and Client Relationships	March 31, 2015

Recommendation 4

The Senior Assistant Deputy Minister, Corporate Services should revise the Security Assessment and Authorization process to take into account the risk associated with the application being implemented.

Management Action Plan	Position Responsible	Completion Date
The Security Assessment and Authorization (SA&A) process will be designed to indicate low, medium or high risk for each information technology application. The Chief Information and Security Officer will provide SA&A expertise to support client-side SA&A requirements. Expected results: Departmental applications and systems will be properly assessed and authorized prior to being deployed.	Senior Assistant Deputy Minister, Corporate Services	March 31, 2015

Recommendation 5

The Senior Assistant Deputy Minister, Corporate Services should implement controls that ensure the Security Assessment and Authorization process is properly completed before the implementation of corporate applications.

MANAGEMENT ACTION PLAN	POSITION RESPONSIBLE	COMPLETION DATE
The management action plans for recommendations 2, 3 and 4 will mitigate this finding. Strengthened communications will help to ensure that project managers understand the Security Assessment and Authorization (SA&A) process. Adoption of the Projects and Client Relationships Branch Project Management Centre of Excellence methodology will establish the necessary gating and controls at each stage in the development of corporate applications. Expected results: Controls are in place to ensure that the SA&A process is properly completed, as required, before corporate applications are deployed.	Senior Assistant Deputy Minister, Corporate Services	March 31, 2015

Annex A: Audit Criteria

The following audit criteria were used in the conduct of this audit:

1. SSC developed and implemented policies and procedures that ensured that security-related activity was established in a manner consistent with existing government policies.
2. Through the conduct of SA&A, SSC addressed security risks associated with using corporate IT systems to support SSC business activities.

Annex B: Acronyms

Acronym	Name in Full
CISO	Chief Information and Security Officer
CS	Corporate Services
CSEC	Communications Security Establishment Canada
DG CITS	Director General, Cyber and Information Technology Security Transformation Program
DSP	Departmental Security Plan
IT	Information Technology
ITS RMF	Information Technology Security Risk Management Framework
MITS	Management of Information Technology Security Standard
PCR	Projects and Client Relationships
PDS	Policy on Departmental Security
PMCoE	Project Management Centre of Excellence
SA&A	Security Assessment and Authorization
SADM	Senior Assistance Deputy Minister
SSC	Shared Services Canada
TB	Treasury Board