



[Canada.ca](#) › [Shared Services Canada](#) › [Publications and reports](#)

Audit of Security Assessment and Authorization

Table of contents

Executive summary.

A. Introduction

1. Background
2. Rationale for the Audit
3. Audit Authority
4. Objective of the Audit
5. Scope
6. Methodology / Approach
7. Statement of conformance

B. Findings, recommendations and management response

1. Governance

- 1.1 IT Security Assessment and Authorization Policy Framework
- 1.2 SA&A Roles and Responsibilities
- 1.3 Oversight

2. Risk

- 2.1 IT Security Risk Management

3. Internal Controls

- 3.1 SA&A Process

3.2 Standard SA&A Reviews

3.3 ATO Condition Monitoring and Authorization Renew

C. Conclusion

Annex A – Specific Lines of Enquiry and Audit Criteria

Annex B – Sample Approach

Annex C – Audit Recommendations Prioritization

Annex D – List of Acronyms

Executive summary

Security Assessment and Authorization (SA&A) is the process by which departments ensure that only authorized software and hardware are implemented in their information technology (IT) environment. Security Assessment is an ongoing process that evaluates security practices and controls to determine if these are implemented correctly, operating as intended, and achieving the desired outcome. Security Authorization involves obtaining and maintaining a security risk management decision which explicitly accepts the related residual risk, based on the results of a security assessment. This authorization is referred to as “the Authority to Operate” (ATO).

Treasury Board (TB) policy ¹ and Shared Services Canada (SSC) departmental ² specify that SA&A must be conducted and periodically reviewed for all departmental IT systems and applications.

The objective of this audit was to provide assurance that Security Assessment and Authorization (SA&A) reviews of IT systems and services are being conducted in accordance with a formal process and in compliance with Treasury Board of Canada (TB) and SSC policy requirements. The SSC governance structure defines two separate entities

that conduct SA&A: Corporate Services is responsible for conducting SA&A for internal systems (Corporate); and, the Chief Technology Officer Branch (CTOB) is responsible for enterprise infrastructure (Enterprise).

SSC's risk management for IT applications and infrastructure makes use of standard artifacts, active risk logging and a risk register to identify outstanding risks related to IT applications and infrastructure. The risk management practices for Enterprise and Departmental SA&A align well with TB policy and related guidance.

The audit team also found that:

- the development of policy instruments and guidance for SA&A has been evolving at a slow pace
- SA&A roles and responsibilities are not up-to-date and are not clearly communicated or understood by SSC Branches or customers
- organizational changes and ongoing resource concerns have had a negative impact on SA&A oversight
- SA&A activities, ATO production and compliance reviews are being reported to senior management, however, while dashboards are being used, information is incomplete and is focused on throughput statistics rather than on analysis and proposed resolutions
- SA&A artifact templates are not always standard as to format and content
- while a set of practices drives the SA&A activity, there is no formal, management approved and communicated SA&A business process for business intake through to ATO conditions reporting
- despite clear indications that the SSC SA&A efforts are delivering outputs, SA&A activities and the issuance of ATOs do not follow consistent practices

- reviews of ATO conditions were not followed in a consistent or standardized manner

The audit team has developed recommendations to address these audit findings. SSC management is expected to develop Management Action Plans to respond to the audit.

Begonia Lojk

Acting Chief Audit and Evaluation Executive

A. Introduction

1. Background

Security Assessment and Authorization (SA&A) is the process of obtaining and maintaining a management decision to authorize operation of an information system or a service and to explicitly accept the residual risk of an agreed-upon set of security controls, and the results of continuous security assessment³. The Security Assessment evaluates security practices and controls to determine if they are implemented correctly, operating as intended, and achieving the desired outcome with respect to meeting defined security requirements. Security Authorization is the security risk management decision to accept the related residual risk and to maintain the security posture on an ongoing basis.

The authority for SA&A is the Treasury Board (TB) *Policy on Government Security* (PGS) and the *Directive on Security Management* (DSM), and its *Mandatory Procedures*⁴, all effective July 1, 2019. PGS subsection 3.2.4, directs departments that “risk-based and standardized security practices and controls will be implemented, monitored and maintained”. The DSM’s *Mandatory Procedures*⁵ states that departments are to “implement IT security assessment and authorization processes”. In addition, SSC

departmental policy addresses the subject of IT security and the relationship to IT applications and services. The 2014 SSC Policy on Departmental Security sets out the requirements that include SA&A approval for all systems and services ⁶. Furthermore, changes or modifications to a system or application affecting the Statement of Sensitivity (SOS) invalidates the previous assessment, thus requiring a re-assessment prior to implementation ⁷. The actual SA&A procedure is described by the ITSG-33 guidance published by the Communications Security Establishment ⁸.

As an internal enterprise services organization ⁹, SSC is mandated to provide IT infrastructure services on an enterprise (that is, whole-of-government) basis to customer organizations that operate IT systems in SSC controlled environments. SSC is responsible for issuing the Authority to Operate (ATO) for the enterprise infrastructure. SSC must also manage the ATOs for its own departmental business systems.

There are two organizations within SCC that are directly involved in SA&A activity. For enterprise environments and services, the Security Management and Governance (SMG) Directorate, Chief Technology Officer Branch (CTOB), carries out the SA&A effort and recommends the ATO with or without conditions to the enterprise authorizer. The Chief Security Officer, Corporate Services Branch (CSB), carries out the SA&A effort for departmental systems and services and is also the departmental authorizer. This SA&A effort is combined with business intake and conditions monitoring to create a concept-to-compliance business lifecycle. As such, enterprise SA&A is triggered by the SMG business intake procedure ¹⁰ and is normally associated with a project to deliver a system or a service using the SSC infrastructure. Departmental SA&A is a cooperative effort between the IT Security staff and project teams reporting to the Chief Information Officer (CIO). Prior to delivery of the final product,

the project is subjected to a security assessment which will identify and assess how IT security controls are incorporated. The Authority to Operate (ATO) is the final step before deployment. If the ATO is issued with conditions, these conditions are then monitored.

The SA&A business process works within the SSC governance committee structure. The Service, Program and Procurement Review Board (SPPRB) mandate includes the approval of cyber and IT standards recommendations and Security Assessment and Authorization recommendations for all new enterprise services ¹¹. The Senior Assistant Deputy Minister (SADM), Service Delivery and Management Branch (SDMB), is the Chair of the SPPRB, and assumes the role of enterprise authorizer. To accomplish this mandated task, the SPPRB relies on advice and recommendations from the Security Risk Management Board (SRMB). SRMB's mandate includes the review, analysis and management of a range of medium to high-risk cyber and IT security issues, and risks that could affect the Government of Canada's IT infrastructure ¹². Specifically, it makes recommendations to the SPPRB during the SA&A process. According to the Departmental SA&A procedure, the CIO is the authorizer.

2. Rationale for the Audit

To improve overall security within the Government of Canada (GoC) IT community, organizations must verify that the security requirements established for a particular system or service are met and must prove that the controls and safeguards are working. This involves identifying and assessing risks to the IT environment, and accepting the residual risk of operating the system or service once identified risks have been mitigated.

A properly set up and functioning SA&A business process can provide management with the confidence that only accepted and authorized IT systems and services are put into operation with appropriate levels of

security. The lack of a properly functioning SA&A business process can impact the delivery of IT services, and result in the acceptance of poorly operating or insecure IT services and systems. Unprotected IT systems and services can result in loss of control over networks or systems, or in the accidental or intentional access to sensitive information.

3. Audit authority

The audit was included in SSC's 2019-22 Risk Based Audit Plan, approved by the President on March 5, 2019. This audit was executed under the authority of the Office of Audit and Evaluation (OAE).

4. Objective of the audit

The objective of this audit was to provide assurance that Security Assessment and Authorization (SA&A) reviews of IT systems and services are being conducted in accordance with a formal process and in compliance with TB and SSC policy requirements.

5. Scope

The scope of this audit focused on the business process for SA&A in SSC, existing ATOs resulting from that process and the extent to which key enterprise and SSC departmental projects are producing required artifacts used in the assessment of IT services and systems. The audit also reviewed business intake and ATO conditions monitoring. The scope covered the period of April 1, 2018 to August 31, 2019.

The audit did not include any attempt to rework actual security assessments, or re-evaluate evidence used during such assessments.

6. Methodology / Approach

The audit was conducted in accordance with the International Internal Audit Standards (IIA) for audit engagements and the Treasury Board of Canada Policy on Internal Audit. The audit was carried out, including the following audit procedures:

1. interviews with operational staff and senior management
2. document reviews
3. walkthroughs of key systems and processes and procedures
4. identification of key controls
5. sampling projects and/or services using a judgemental sampling technique
6. data analysis
7. controls testing

7. Statement of conformance

In my professional judgment as Chief Audit Executive, sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the opinion provided and contained in this report. The opinion is based on a comparison of the conditions as they existed at the time against pre-established audit criteria that were agreed to with management. The opinion is applicable only to the entity examined. The engagement was conducted in conformance with the requirements of the Policy on Internal Audit, its associated directive, and the IIA Code of Ethics. The evidence was gathered in compliance with the procedures and practices that meet the auditing standards, as corroborated by the results

of the quality assurance and improvement program. The evidence gathered was sufficient to provide senior management with proof of the opinion derived from the internal audit.

B. Findings, recommendations and management response

1. Governance

1.1 IT Security Assessment and Authorization Policy Framework

Audit criterion: SSC has developed, approved, communicated and updated a Policy / Directive on the assessment and authorization of IT systems and services, prior to implementation, and as an ongoing process after implementation.

We expected to find an existing policy framework covering security assessment and authorization (SA&A) and a set of formal documents outlining how the policy framework was to be implemented. We also expected to find that staff responsible for carrying out SA&A-related tasks were knowledgeable in implementing the guidance, and that clients of the process were aware of the policy, the guidance and the requirements of SA&A.

A complete and up-to-date policy framework ensures the development and enforcement of a formal process that meets SSC's mandate as an internal enterprise service organization, and outlines the need to communicate this requirement to all stakeholders.

Recent changes to government policy have highlighted the need for security assessment and authorization ¹³. SSC has published several policy and directive documents that address this central government requirement and provide a solid policy basis for SA&A, which is part of the government and departmental view of cyber and IT security risk management. Two parallel business processes are in place to address SA&A, one for the departmental applications and the other for enterprise infrastructure systems and services. There is, however, no prescribed, definitive and approved process guidance available that covers the business of SA&A from intake to conditions monitoring. The Departmental Security Plan (DSP) (2019-22) indicates that organizational change may have resulted in a lack of understanding of actual task assignments, and suggests that policy, directive and process updates are needed ¹⁴. The audit team noted that:

- guidance documents that address some process aspects of SA&A are undated, without reference to a specific author or any indication of approval, inconsistently worded and either out of date or in draft. The Chief Technology Officer Branch has been working on an update to the SA&A Security Standard, used currently as guidance for Enterprise SA&A. Updating of this standard started in 2016; it has not been published yet, and
- the policy and related guidance have not been communicated to SSC staff. Most interviewees not directly involved with the process indicated a general lack of awareness of SA&A requirements, evidence, costs and timeframes.

SSC has published several policy and directive documents that reiterate the GoC position on SA&A. Sufficient business process guidance, however, has not been generated or maintained to implement this policy framework. Insufficient policy implementation guidance will likely lead to

inconsistencies in how the policy is implemented. Furthermore, the lack of communication on the policy guidance to all stakeholders compounds the risk that they may not comply with the requirements.

In conclusion, SSC's policy instruments for the management of security assessment and authorization are incomplete, and not communicated to all stakeholders.

See Recommendation 4.

1.2 SA&A Roles and Responsibilities

Audit criterion: Roles and responsibilities for SA&A are documented, assigned, and communicated to all relevant SSC stakeholders and customers, and functioning as defined.

We expected to find that roles and responsibilities for SA&A were documented and communicated to all stakeholders, particularly to staff who manage and execute SA&A-related tasks. We also expected to find that other related stakeholders had been informed and were aware of their roles in the process.

SA&A-related roles and responsibilities with their related authority need to be communicated and clearly understood by all stakeholders. This helps ensure that participants are aware of and fulfill their responsibilities in the process.

In a general sense, the roles are well understood within the organizations involved in SA&A, namely the Chief Security Officer (CSO) for Departmental and the Chief Technology Officer Branch (CTOB) for Enterprise. The audit team found, however, that departmental SA&A uses the SA&A Guide (2016) as procedural guidance, whereas enterprise SA&A follows the SA&A (draft) Standard. In addition, the audit team found that:

- Role descriptions are different between departmental and enterprise SA&A functions. The Departmental Security Plan indicated that there may be gaps in SSC's security controls or management framework as a result of lack of clarity regarding security governance, roles and responsibilities, both within the department and with its customers and other external stakeholders ¹⁵.
- The enterprise Compliance organization was set up in August 2018 to monitor and report on ATO conditions. Procedural documentation for this function is weak.
- ITSG-33 ¹⁶ Annex 2 outlines steps for implementing security controls in information systems. Annex 3 provides a catalogue of security controls containing definitions that security practitioners can use to select specific controls to protect GoC systems and IT services. ITSG-33 offers no definition of Security Practitioner (assists project in finding evidence) versus that of Security Assessor (measures the quality of evidence). This may result in not having the implementation of security controls and the measurement of that implementation properly segregated.
- The assessor vs. authorizer roles for corporate services and enterprise services, for department-specific and for whole-of-government, are not clear. For example, although the DSP in February 2019 cites the Executive Vice-President as the authorizer for enterprise ATOs, the most recent Terms of Reference for the Service, Program and Procurement Review Board (SPPRB) indicates that the Senior ADM Service Delivery and Management Branch has taken on this role.
- This may be why interviewees indicated that role clarity and enforcement of responsibilities in certain areas is weak.

If SA&A roles are not well defined or documented, there is a risk that segregation of duties between the security practitioner and the assessor are unclear, thereby compromising the validity of the assessment result. Furthermore, if roles and responsibilities are not communicated or clearly understood, there is a risk of duplication of effort and of confusion.

In conclusion, the audit found that roles and responsibilities for SA&A are not well documented, and not formally communicated to all relevant stakeholders within SSC.

Recommendation 1

Medium priority

The Senior Assistant Deputy Minister/Chief Technology Officer Branch and the Senior Assistant Deputy Minister Corporate Services Branch (via the Chief Security Officer), should clarify the mandate for IT security assessment for both corporate and enterprise environments and ensure that roles and responsibilities are established and communicated to all stakeholders.

Management response

Currently there are policy instruments being developed/updated based on expectations set-out in the renewed Treasury Board Secretariat (TBS) Policy on Government Security (PGS) ¹⁷ and associated Directive on Security Management (DSM) ¹⁸. SSC's Policy on Departmental Security (PDS) ¹⁹ is being revised to clarify roles and responsibilities. The President has designated

a CSO in the CSB to oversee departmental security management activities, and SSC is investigating what other changes are required to align with the PGS as it pertains to the delivery of SSC Enterprise Services. Furthermore, the SSC Directive on Security Management for Enterprise Services ²⁰ (currently DRAFT) will define clear and specific roles and responsibilities for IT Security as it pertains to delivery of enterprise services.

1.3 Oversight

Audit criterion: There is an effective oversight regime in place to manage the security assessment and authorization (SA&A) of IT systems/services.

We expected to find an oversight regime in place that included a governance structure, management and direction, funding, and monitoring and reporting for SA&A.

Efficient and effective oversight ensures that departmental IT security requirements and objectives are aligned with the TB *Policy on Government Security* and *the Directive on Security Management* and that business strategies, direction and key risks for delivering on the departmental mandate have been identified and are appropriately controlled.

As noted earlier, SSC has two separate but related management functions directing SA&A activities: the internal, corporate (departmental) function responsible for SSC corporate systems, under the purview of the Corporate Services Branch; and, the Chief Technology Officer Branch (CTOB) for Enterprise (whole-of-government) IT, where SSC is the internal enterprise services organization for government IT infrastructure.

The audit team noted that:

- There are differences between enterprise and departmental SA&A activities, such as respective mandates and scope (dollars, extent of work, etc.). Although the Departmental Security Plan attempts to address enterprise issues, the source documentation supporting these enterprise issues could not be found. There is no equivalent enterprise security plan that has been formally articulated or defined, which means that enterprise issues are not being addressed.
- In both departmental and enterprise organizations involved in SA&A, there is a lack of sufficient capacity to achieve the workload mandated by government policy. This is resulting in delays, backlogs and customer concerns. The departmental SA&A operation is very small and the workload is often managed informally. Enterprise SA&A is a much larger operation. The audit team noted that the IT Security Risk Assessment Services unit responsible for the enterprise Security Assessment activity is thinly staffed and relies heavily on contracted resources for security practitioners and security assessors. In addition, the enterprise Security Compliance unit, responsible for monitoring and reporting on compliance to authorized operating conditions, was set up and operates as a net new function for which no new resources were added.
- The cost recovery funding model does not meet the needs for the internal control requirements for SA&A. Cycle time from initial assessment to recovery of costs can be substantial; these are estimated at over 9 months²¹. SA&A is a demand-driven activity yet there appears to be no easy way at SSC to ensure SA&A work can be proactively funded to secure appropriate resources in a timely manner to ensure SA&A work is not constrained.

- Overall, the governance structure is not adequately formalized. The documents are undated and do not have approval signatures. The Terms of Reference for the key governance committees – Service, Program and Procurement Review Board (SPPRB), and the Security Risk Management Board (SRMB) have not been approved by the President.
- The SRMB underwent an organizational change sometime after December 2018. This Director General-level committee focuses on security risk management and, among other agenda items, receives reports concerning SA&A workload, statistics and issues. The SRMB co-chairs of the re-constituted committee had not determined the appropriate information, and the visibility for SA&A within SSC is not optimal.
- Reporting on the security status of enterprise information systems to the authorizing official, business owner and other stakeholders on an ongoing basis, in accordance with SSC's continuous monitoring strategy and the system's authorization plan, is defined in the *SA&A Security Standard* (Draft) ²². All enterprise SA&A managers are required to update weekly dashboards. These dashboards are then bundled to represent the work accomplished for the week. The audit team noted that no trend analysis was being conducted for this standard reporting instrument. Risks and issues identified in the dashboards highlight symptomatic concerns, however, there was no overall reporting on how many projects are experiencing delays, or evidence of ongoing dialogue on the results of the suggested actions needed to address the risks or issues.
- There is a lack of rigour in the capture and reporting of key indicators in conveying enterprise security assessment project delays, in reporting horizontal risk aggregation ²³ from SA&A analyses, and in reporting escalation options for non-compliance.

Due to these deficiencies in SSC's oversight for SA&A, there is a risk that the lack of capacity will result in workload delays and deployment backlogs, that funding issues will lead to ineffective internal controls in the SA&A process, that governance structures are not sufficiently responsive to SSC's changing enterprise security role, and that inadequate reporting will limit effective management decision-making. These concerns pose a risk to SSC's business reputation as a trusted internal enterprise services organization.

In conclusion, there is inadequate oversight on the management of security assessment and authorization.

Recommendation 2

 High priority

The Senior Assistant Deputy Minister/Chief Technology Officer Branch and the Senior Assistant Deputy Minister Corporate Services Branch (via the Chief Security Officer) should ensure that an effective oversight regime is in place to:

1. implement a formally approved and adequately staffed organization to allow both SA&A streams to meet their ongoing mandated activities in a cost-effective and customer-focused manner
2. establish and ensure an appropriate funding mechanism such that enterprise and departmental SA&A can organize to meet workload requirements with predictable output results

3. revise and finalize an approved governance structure, including committee (SRMB) Terms of Reference and membership in support of SSC reputation as an internal enterprise services organization in the SA&A context
4. define what level of monitoring and reporting is expected and what type of enterprise and corporate security information for the management of SA&A is required to enable effective senior management decision-making.

Management response

Management agrees with the recommendation.

CTOB Security Management and Governance and the CSO will review its current organisational structure and staffing levels to ensure it is properly resourced to meet ongoing mandated activities in a cost-effective and customer-focused manner. Efforts will be taken to ensure sufficient full time employees that are trained to provide consistent and cost effective SA&A services. This will include running a selection process to staff positions, updating the organisational structure to improve service delivery, revising the funding model to meet interim workload requirements and improving the governance structure by reporting to the Security Risk Management Board (SRMB).

Recommendation 3

Medium priority

The Senior Assistant Deputy Minister/Chief Technology Officer Branch should establish a planning framework to permit enterprise issues to be identified, researched and addressed in a manner similar to that of the Departmental Security Plan.

Management response

Management agrees with the recommendation.

According to the PGS, the DSP is intended to cover all departmental programs and services. Consequently, the SSC DSP addresses both corporate and Enterprise services. There are also requirements under the Treasury Board Policy on Service and Digital (coming into effect April 1, 2020) for integration of cyber security within a departmental plan for the integrated management of service, information, data, information technology, and cyber security. Together, these plans will provide strategic direction for improving the security of SSC Enterprise Services, in accordance with government-wide priorities.

2. Risk

2.1 IT Security Risk Management

Audit criterion: There is a process to identify and monitor security risks of all projects throughout their lifecycle with respect to: the use of standard risk artifacts addressing the IT security risk aspects of ITSG-33; the use of active logging and monitoring of IT security risk artifacts; the use of an IT risk register that includes risk identification and a mitigation strategy for managing IT security risks.

We expected to find that SSC has:

- implemented active logging and monitoring of projects (infrastructure and applications)
- conducted routine assessments of security risks for identified projects
- developed an IT risk register that includes risk identification and a mitigation strategy for managing IT security risks

Project managers and sponsors need to be aware of the evolution of the threat and risk landscape and understand how to manage their IT security risks. To this end, projects are expected to utilize ITSG-33 controls and steps to identify required security controls, and determine how well these controls have been implemented within the business solution being developed. Implementing and maintaining a register for IT security risks provides SSC project managers with an awareness of the evolving IT security risks. The expected risk register should also track risk mitigation measures.

SSC's security risk management for IT applications and infrastructure makes adequate use of standard artifacts, active risk logging and risk reporting to identify outstanding risks involving IT applications and infrastructure. Nevertheless, there are discrepancies in current and the draft documents which describe the artifacts and the expected evidence such as:

- Departmental SA&A follows the SA&A Guide (2016) whereas Enterprise SA&A follows the SA&A Standard (which is yet to be finalized). Each group uses slightly different templates to produce the required artifacts. Not all templates reside in the same repository, and several source documents offer a partial exploration of which artifacts are to be used and where. This situation results in a confusing set of instructions.
- Project managers who produce the evidence to address required artifacts are not aware of the existence of a formal process; they simply use whatever list of artifacts is provided by the SA&A function. Although most see SA&A artifacts as natural outcomes of good project management, they do not understand the requirement for artifacts, making it difficult for them to provide appropriate evidence.

Inadequate implementation of standard artifact templates has adversely impacted SSC's ability to control the quality of artifact completion and limits the ability to compare these documents.

In conclusion, procedures for active logging and monitoring, and the provision of a risk register are sufficient, however, a standard set of acceptable artifacts with appropriate usage instructions is not available.

(See recommendation 4)

3. Internal Controls

3.1 SA&A Process

Audit criterion: A standard SA&A process has been formally documented, communicated and is integrated with the Project Governance Framework (PGoF).

We expected to find documented, approved, implemented and communicated procedures for managing security assessment and authorization.

A single authoritative source for the SA&A process at SSC would prevent extreme variability in levels of proof for specific ATOs, and ensure that ATOs are revoked when necessary. A formal communications vehicle for project managers regarding SA&A objectives, artifacts, etc. would help ensure an effective SA&A process. Process uncertainty can necessitate a major coordination effort on the part of SA&A teams, resulting in process inefficiencies.

The Communication Security Establishment's ITSG-33 provides a baseline set of control activities and actual security controls to be applied to a project delivery – either application or infrastructure. The practices covering both Enterprise and Departmental SA&A align well with ITSG-33. In addition, the SSC Project Governance Framework (PGoF) describes a set of project approval gates and cites on a Gate Checklist many of the artifacts used as evidence for SA&A assessment. There is, however, insufficient formal business process documentation for SA&A activities. The audit team found that:

- Two guidance documents exist – the SA&A Guide, an older document dated 2016 for which a rework exists in draft, and the draft SA&A Security Standard. Ideally the two streams should be different elements of the same process. These two streams, however, represent different sets of practices, which potentially results in inconsistencies in the security assessment discipline.
- There is no single authoritative source for SA&A standards and guidelines. While several documents exist, there are inconsistencies among them. The draft SA&A Security Standard has been in development since 2016, and is scheduled for publication in January

2020. A number of presentation decks (circa 2017-18) describe the Enterprise SA&A process and how it relates to Project Management and delivery. These decks are not authoritative documents. Also, the SA&A Guide (May 2016) states that it provides an overview of the Shared Services Canada *IT Security Risk Management Framework* (SSC ITS RMF). This document is no longer in use for enterprise projects. Furthermore, the SA&A Guide describes responsibilities and the production of key artifacts, which are not always the same artifacts used for the enterprise functions.

- The draft Standard indicated that some older PGoF ²⁴ references were inaccurate, which will require greater effort to align the two frameworks. Similarly, the departmental process makes use of the SA&A Guide which also describes stages of IT project management with reference to SA&A interfaces and outputs, but as PGoF is enterprise focused, with no alignment evident.
- In the absence of a communications program, SA&A managers are expected to communicate SA&A policy and process matters to stakeholders, however, SA&A communications is not considered a priority and presents a challenge for managers already busy with SA&A operations.

The SA&A procedure outlined in the ITSG-33 set of documents deals with the specifics of integrating security controls into the system or service delivery. For example, it includes procedure for defining business needs for security, tailoring security controls, incorporating and testing security controls, then assessing that controls have been suitably tailored, incorporated and tested. This audit took a broader view of SA&A in that it also regarded business intake, the assignment of appropriate resources and ongoing conditions monitoring. The audit team noted that:

- The DSP (2019-22) raised several concerns including: inconsistent processes between enterprise and departmental systems; [This information has been severed] ²⁵; and, legacy systems that have undergone major changes since first being authorized after being transferred to SSC.
- It is not known if all project-sized investments are acknowledged as projects and are captured for SA&A. Enterprise business (that is to say, projects) arrive via the Business Intake unit, from direct contact with the Director, IT Security Risk Assessment Services (ITSRAS) or simply recognized as a requirement. If projects do not use PGoF or do not go through the Business Intake point, there is nothing in place to notify or trigger the project to engage SA&A services. Departmental business is often identified informally between the SA&A coordinator and the CIO staff.
- A trigger for following up on changes to existing services and systems does not exist. There is no requirement for a user making the change to bring it to the attention of compliance and to reassess the ATO.
- When the legacy infrastructure was transferred to SSC, it was assumed, by default, it was authorized to operate, although there is no documented evidence to support this. Both SA&A staff and service line staff indicated that there is ongoing change to legacy environments, where SSC has agreed to the “lift and shift” of [This information has been severed]
- The Enterprise authorizer relies on signoffs from the CTO and business owners. The CTO signs off on the SA&A process, and business owners sign off on ATO conditions which include plans to review and mitigate risks. There is minimal support for the authorizer role, for example: completeness of the ATO packages received varies; time pressures for

authorization signoffs result in a sense of urgency in every case; and, lacking direct governance review of ATO risks and conditions.

Despite clear indications that the SA&A process is delivering outputs, the concerns identified regarding SA&A activities and issuance of ATOs indicate that the process is inefficient. The lack of standardization such as the inconsistencies in application of procedures and differences in requirements for the interpretation of evidence are weaknesses in the process. SA&A process failures may allow ATOs to be issued in error. The differences in processes for corporate and enterprise can result in ATO decision making that is not optimal and [This information has been severed] ²⁶ Formalizing processes and communicating them to staff and partners would lessen the risk of accepting higher residual risk.

In conclusion, SSC has not implemented or documented consistent procedures for the management of security assessment and authorization throughout the Department.

Recommendation 4

 High priority

The Senior Assistant Deputy Minister/Chief Technology Officer Branch and the Senior Assistant Deputy Minister Corporate Services Branch (via the Chief Security Officer), should ensure that sufficient guidance is developed, approved and promulgated for the assessment of security risks and the authorization of systems and services by:

- formalizing and harmonizing processes and procedures to carry out SA&A on corporate and enterprise systems and services

- ensuring all work that requires SA&A is collected, and the risk of not determining the entire SA&A landscape is assessed
- determining the risk to SSC of the legacy environment and systems
- improving support for the authorizer by ensuring the status of all ATO packages are reviewed at SRMB
- establishing formal training and regular communications concerning the SA&A process operations
- implementing common templates to meet the requirements of ITSG-33 across the Department.

Management response

Management agrees with the recommendation.

As per response to recommendation 1, an SSC Directive on IT Security Risk Management ²⁷ and an SA&A standard will be developed jointly by CTOB and CSB. This will contribute to harmonizing processes and procedures for carrying out SA&A on corporate and enterprise systems and also ensure the risk landscape is better understood.

This SSC Directive on Security Management and the SA&A Standard will address the maintenance of SA&A information for all infrastructure (including consideration for legacy infrastructure) under the responsibility of SSC. It will also outline the governance

for review of ATO packages at SRMB to reinforce the authorization process. The SMG Business Oversight Office will further develop its processes to better integrate into enterprise business intake and the project management gating framework in order to ensure that all applicable SA&A is captured and addressed.

Training requirements for individuals involved in the SA&A process are to be addressed as part performance management, in accordance with SSC human resources management processes. Finally SA&A templates will be reviewed and revised to ensure common and consistent alignment to ITSG-33 processes.

3.2 Standard SA&A Reviews

Audit Criterion: SSC applies a standard set of triggers and SA&A procedures to identify, capture and assess all appropriate projects, and authorize all resulting IT systems and service.

We expected to find that security assessments were conducted in a standard manner, following consistent and documented processes to deliver trusted results.

Collection of evidence collection is the heart of the SA&A process. Evidence is required to confirm that each security control (requirement) is in place and traceable. The burden of proof to demonstrate that the designed control exists and is functioning correctly is on the project implementation team. The onus should not be on the Security Assessor to find holes in the evidence. The artifacts ²⁸ created by the assessment team must thus

provide a high level of quality, consistent formatting, the presence or absence of dependent artifacts, clarity on decisions, completeness, currency and accuracy and clearly stated roles that demonstrate the responsibility for evidence.

The sampled SA&A artifacts demonstrated that the timeliness, clarity and completeness of documentation for enterprise security assessments are generally inadequate. For more on the sample approach, refer to Annex B. Sample results show:

- Some products are in operation without a formal ATO. For example:
 - VMWare Refresh Project: Successive upgrades and updates to the VMWare software were installed while being subject to security assessment activity, yet no authorization had been issued.
 - Administrative Access Control Service (AACS): Three modules were involved: Admin Module (AM); Change Auditor (CA); Privileged Access Management (PAM). The audit team did not find SA&A documentation for AACS-AM to indicate the module was officially exempted (at business intake or otherwise) from SA&A. AACS-AM had already passed Gate 4 (deployment) and was approaching Gate 5 (Deployment Completed). No ATO existed for AACS-AM. AACS-CA had already passed Gate 4 (Deployment) and was approaching Gate 5 (Deployment Completed). An ATO had been issued. AACS-PAM was proceeding to Gate 4. Assessment was still underway. No ATO had been issued.
- The audit team noted that the GCDOCS folder structure for enterprise SA&A, which demonstrated some common elements across projects was generally poorly organized, with some randomness across SA&A projects. Departmental SA&A folders were also similarly poorly organized.

- System and service Project Managers indicated that SA&A requests for evidence and the assessment of that evidence changes depending on the individual from enterprise SA&A involved. They also noted that evidence gathered from across projects was not centralized, resulting in duplication of work and ensuing frustration dealing with several requests for the same evidence.

Without a standardized methodology or formal procedures for SA&A practices, SSC is at risk of not being able to demonstrate rigour of security assessments and the resulting authorization of services or systems operating on the enterprise IT infrastructure, thus adversely impacting SSC's reputation and the public/client trust in SSC.

In conclusion, there is no standardized SA&A methodology, no triggers or procedures to identify, capture and assess all appropriate projects, and to authorize all resulting IT systems and services in both the enterprise and departmental SA&A functions.

Recommendation 5

Medium priority

The Senior Assistant Deputy Minister/Chief Technology Officer Branch and the Senior Assistant Deputy Minister Corporate Services Branch (via the Chief Security Officer) in collaboration with the Senior Assistant Deputy Minister Service Delivery and Management, should address the challenges in the SA&A process, specifically:

- reviewing inconsistencies in SA&A practices, which result in differences in the evidence requested and assessed

- ensuring evidence is collected only once and re-used as necessary
- implementing a well-organized central design for all SA&A GCDOCS folders

Management response

Management agrees with the recommendation.

An SSC Directive on IT Security Risk Management and a SA&A standard will be developed jointly by CTOB and CSB to ensure a consistent and organised approach to SA&A processes, procedures and practices. CTOB will also introduce a new governance risk and compliance management solution (RSA Archer) that will introduce automation and increased efficiency of the SA&A process while also ensuring consistency between the teams and their practices.

3.3 ATO Condition Monitoring and Authorization Renewal

Audit criterion: SSC has implemented a process to review and revise ATOs for services or systems to verify that authorizations continue to be valid, and uses standard triggers to ensure ongoing compliance with ATO conditions and requirements.

Part of the overall security assessment and authorization function is to monitor when ATOs are issued with conditions, and to ensure that conditions are met. We expected to find that reviews of ATO conditions were approached in a standard manner, following consistent processes.

Government of Canada and departmental policies require the monitoring of conditions and re-assessment of security risks, as necessary. In particular:

- Security Assessment and Authorization (SA&A) must be conducted and periodically reviewed for all departmental IT systems and applications, and ²⁹
- Changes or modifications to a system or application affecting the data Confidentiality, Integrity, and Availability (CIA) values, as identified in the Statement of Sensitivity (SOS), will invalidate the previous SA&A and require a re-assessment prior to implementation. ³⁰

Conditions monitoring has been weak for enterprise and departmental SA&A functions. The audit team noted that:

- For enterprise, the compliance organization was set up in August 2018 and remains very small, comprising a manager, one staff member and one student. There was no organizational chart, and overall governance was not documented. A formal hand-over process between the assessment group (ITSRAS) and the compliance group was under development. Departmental SA&A carried out some monitoring but, due to a very small staff size, there was no segregation of duties between assessment and compliance.
- Continuous monitoring had not been fully implemented for enterprise ATOs and was carried out by the same people who perform SA&A duties for departmental ATOs. Once the service was allowed to “go live” there was nothing in place to convince service and system owners of the need to complete or obtain an ATO. If there was no ATO (or conceptually if an ATO is revoked), the service was not shut down.
- The range of consequences for non-compliance resulting from ATO condition monitoring was yet to be determined. Management was

unsure about what could be done once the service or system was in operation. Although this could be changed, it was noted that Some systems had limited tolerance for a shut down.

- Condition reporting is a crucial component of compliance monitoring. With the implementation of more standard processes, enterprise teams have begun to track associated conditions. Currently, no enterprise ATO is signed if the conditions do not have an OPI, lack a signature from the owner's Senior Management and are missing a scheduled completion date.
- Analysis of ATOs granted to date was lagging for older ATOs. No formal escalation process existed. While service lines owners were seen as accountable for meeting ATO conditions, these owners did not follow up regularly, and there was no evidence of enforcement action to deal with expired ATOs (interim ATOs and final ATOs with conditions).

Enterprise and departmental compliance activity, via monitoring and enforcement, does not have the capacity or the management support to effectively ensure that GoC systems and services are sufficiently protected from potential threats. As a result, SSC is not meeting the policy directive of ongoing monitoring and re-authorization.

Recommendation 6

Medium priority

The Senior Assistant Deputy Minister/Chief Technology Officer Branch and the Senior Assistant Deputy Minister Corporate Services Branch (via the Chief Security Officer), should implement a standardized process for monitoring and enforcing ATO conditions.

Management response

Management agrees with recommendation.

As per response to recommendation 1, a Directive on IT Security Risk Management and an SA&A standard will be developed jointly by CTOB and CSB. These policy instruments will identify responsibilities for monitoring, reporting and compliance to the Security Risk Management Board on the status of SA&A activities and compliance of ATO conditions.

C. Conclusion

SSC has two distinct SA&A responsibilities: corporate (Departmental) and internal enterprise service organization (Enterprise). The governance structure defines two separate entities that conduct SA&A: Corporate Services for SSC corporate systems; and, the Chief Technology Officer Branch (CTOB) for Enterprise IT. This has led to the development of two separate yet related sets of documented guidance, artifact templates and work practices.

Security assessment reviews are conducted by both departmental and enterprise staff following the ITSG-33 guidance. The authorizer role has been assigned in both cases, and ATOs are being signed. ATO condition compliance and monitoring is less managed. In addition, there is a lack of a formal process for ensuring compliance with TB and SSC policies.

SSC exhibits weaknesses in formal guidance documentation, coordinated SA&A approaches between departmental and enterprise, standardization of templates, and a common set of work practices. This has resulted in the lack of understanding of roles and responsibilities. Recent and ongoing governance changes have resulted in organizational and capacity issues for both environments not being addressed in a timely fashion.

The lack of up-to-date, formalized documentation for the work process, places more reliance on the format and content of the templates for the artifacts used in the assessment and authorization of systems and services. Differences in the templates used for departmental and enterprise adds unnecessary complexity. It also results in duplication of work vis-à-vis requests for evidence and the assessment of that evidence, which is also subject to variability depending on the individual doing the work. There is no assurance that the required SA&A is being conducted for all projects or non-project work.

Until August 2018 the ongoing enterprise monitoring function was co-housed with assessment. This is still the case for departmental SA&A. The enterprise monitoring function is being separated but procedures to manage that effort are still under development. The lack of a formal escalation process combined with the lack of enforcement action results in a heightened monitoring risk.

The differences that exist between enterprise and departmental SA&A include timeframes, scope, resources, and customer involvement. Although the Departmental Security Plan attempts to address enterprise issues, the source documentation supporting these enterprise issues was not found. There is no provision for a plan that deals with enterprise issues.

A common formal process is needed with separate implementations to address the differences between departmental and enterprise SA&A. The current evolution of separate SA&A processes and practices is inefficient

and poses challenges to the proper application of best practices for the management of security assessment and authorization.

Annex A – Specific Lines of Enquiry and Audit Criteria

Audit of Security Assessment and Authorization

Criterion Title	Audit Criterion
Line of Enquiry 1: Governance ¹ ² ³ ⁴	
1.1 IT Security Assessment and Authorization policy framework	SSC has developed, approved, communicated and updated a Policy / Directive on the assessment and authorization of IT systems and services - prior to implementation, and as an ongoing process after implementation.
1.2 SA&A Roles and responsibilities	Roles and responsibilities for the Shared Services Canada SA&A process are documented, assigned and communicated to all relevant SSC stakeholders and customers, and functioning as defined.
1.3 Oversight	There is an effective oversight regime in place to manage the security assessment and authorization (SA&A) of IT systems/services.
Line of Enquiry 2: Risk Management ³ ⁸	
2.1 IT Security Risk Management	There is a process to identify and monitor IT security risks of all projects throughout their lifecycle with respect to: using standard risk artifacts (ITSG-33); active logging and monitoring of IT security risks on projects; and, using a risk register for managing IT security risks.

Criterion Title	Audit Criterion
Line of Enquiry 3: Internal Controls <u>1</u> <u>3</u> <u>4</u> <u>5</u> <u>6</u> <u>7</u> <u>9</u>	
3.1 SA&A and Project Management integration	A standard SA&A process has been formally documented, communicated and is integrated with the Project Governance Framework (PGoF).
3.2 Standard SA&A reviews	SSC applies a standard set of triggers and SA&A procedures to identify, capture and assess all appropriate projects, and authorize all resulting IT systems and service
3.3 ATO condition monitoring and authorization renewal	SSC has implemented a process to review and revise ATOs for services or systems to verify that authorizations continue to be valid, and uses standard triggers to ensure ongoing compliance with ATO conditions and requirements.

Sources of criteria

- 1 Shared Services Canada - *Policy on Departmental Security*, May 1, 2014.
- 2 Treasury Board of Canada - *Directive on Departmental Security Management*, July 1, 2009
- 3 Communications Security Establishment - *ITSG-33 Annex 3a Security Control Catalogue*, December 2014
- 4 Shared Services Canada - *IT Security Risk Management Directive*, September 17, 2015

- 5 Shared Services Canada - *SA&A Security Standard*, TBD (2019).
 - 6 Communications Security Establishment – *ITSG-33 Annex 2 Information Systems Security Risk Management Activities*, November 2012
 - 7 Shared Services Canada - *SAA Landing Page*, Undated
 - 8 Shared Services Canada - *Project Risk Management Process*- January 2016
 - 9 Shared Services Canada - *Departmental Security Plan V3.1*, February 20, 2019
-

Annex B – Sample Approach

From a population of 39 current enterprise SA&A projects and 12 departmental SA&A projects, the audit team extracted a judgemental sample of 7 and 2 projects respectively. To ascertain the robustness and consistency of the SA&A methodology in place, the audit team examined 6 key enterprise SA&A artifacts (4 for departmental SA&A) for each of the sampled SA&A projects, according to the following dimensions:


- quality of the artifact, compared to the respective template
- format of the artifact, compared to the respective template
- presence or absence of certain artifacts
- decision made
- completeness, currency and accuracy
- roles or RACI charts to show custody of evidence



The enterprise sample represented a cross-section of environments, comprising 4 Enterprise Data Centre projects, 2 Cloud projects and 1 Legacy (customer-led) project. In addition the sampled projects were drawn from the SMG status report and reflected 3 Red (At critical risk), 3 Green (On track) and 1 Yellow (At risk). The departmental sample consisted of one completed assessment and one in-progress.

Annex C – Audit Recommendations Prioritization

Internal engagement recommendations are assigned a rating by OAE in terms of recommended priority for management to address. The rating reflects the risk exposure attributed to the audit observation(s) and underlying condition(s) covered by the recommendation along with organizational context.

Recommendations legend

Rating	Explanation
 High priority	<ul style="list-style-type: none">• Should be addressed as priority for management (that is, within the next six to 12 months)• Controls are inadequate. Important issues are identified that could negatively impact the achievement of organizational objectives• Could result in significant risk exposure (for example, reputation, financial control or ability to achieve Departmental objectives)• Provide significant improvement to the overall business processes

Rating	Explanation
 Medium priority	<ul style="list-style-type: none"> • Should be addressed over the next year or reasonable timeframe • Controls are in place but are not being sufficiently complied with. Issues are identified that could negatively impact the efficiency and effectiveness of operations • Observations could result in risk exposure (for example, reputation, financial control or ability of achieving branch objectives) or inefficiency • Provide improvement to the overall business processes
 Low priority	<ul style="list-style-type: none"> • Changes are desirable within a reasonable timeframe • Controls are in place but the level of compliance varies • Observations identify areas of improvement to mitigate risk or improve controls within a specific area • Provide minor improvement to the overall business processes

Annex D – List of Acronyms

Term	Definition
AACS	Administrative Access Control Service
AM	Administration Module (of AACS)

Term	Definition
ATO	Authority to Operate
BR	Business Request
BRD	Business Requirements Document
CA	Change Auditor (module of AACS)
CCCS	Canadian Centre for Cyber Security
CIA	Confidentiality, Integrity and Availability
CI-CSO	Chief Information & Chief Security Officer
CSO	Chief Security Officer (SSC)
CTOB	Chief Technical Officer Branch (Formerly CITS) (SSC)
DSM	Directive on Security Management (TBS)
DSP	Departmental Security Plan
EDC	Enterprise Data Centre
GCDOCS	Government of Canada Document Management System
GoC	Government of Canada
IESO	Internal Enterprise Services Organization (that is, government department that provides service to whole-of-government)
IIA	Institute of Internal Auditors
IT	Information Technology
ITSG-33	Information Technology Security Guidance – 33

Term	Definition
ITSRAS	Information Technology Security Risk Assessment Services (SMG)
ITSRMF	Information Technology Security Risk Management Services Framework
NSDS	Network, Security and Design Services Branch (SSC)
OAE	Office of Audit and Evaluation (SSC)
OPI	Office of Primary Interest
PAM	Privileged Access Module (of AACS)
PGoF	Project Governance Framework
PGS	Policy on Government Security
PM	Project Manager
PMDB	Project Management & Delivery Branch (SSC)
POAM / POA&M	Plan of Action and Milestones (Formally referred to as the SAP)
SA&A /SAA	Security Assessment and Authorization
SADM	Senior Assistant Deputy Minister
SDMB	Service Delivery Management Branch (SSC)
SMB	Senior Management Board (SSC)
SMG	Security Management and Governance (CTOB)
SoS	Statement of Sensitivity
SPPRB	Service, Projects and Procurement Review Board (SSC)

Term	Definition
SRMB	Security Risk Management Board (SSC)
SSC	Shared Services Canada
TB(S)	Treasury Board (Secretariat)

Footnotes

- 1 TB *Policy on Government Security* (July 1, 2019), *Directive on Security Management* (July 1, 2019).
- 2 SSC *Policy on Departmental Security*
- 3 SSC *SAA Security Standard* 1.2
- 4 TB *Policy on Government Security* (July 1, 2019), *Directive on Security Management* (July 1, 2019).
- 5 DSM's Mandatory Procedures Appendix B, for Information Technology Security Control, subsection B.2.6, states that departments are to "implement IT security assessment and authorization processes to establish and maintain confidence in the security of information systems that are used or managed by the department, while considering stakeholder security requirements"
- 6 SSC *Policy on Departmental Security* 8.1.1 SA&A must be conducted and periodically reviewed for all departmental IT systems and applications

- 7 *SSC Policy on Departmental Security 8.1.2*
- 8 Communications Security Establishment Canada (CSEC) Information Technology Security Guidance – IT Security Management: A Lifecycle Approach (ITSG-33)
- 9 PGS Appendix B – internal enterprise service organization (organisation de services internes intégrés). A department or organization that provides internal enterprise services to other Government of Canada departments. This includes lead security agencies that deliver government-wide security services.
- 10 Note that the SMG business intake procedure deals with all SMG business requests, not just SA&A.
- 11 Final SPPRB Chair Approval (TOR) dated May 28/2019
- 12 Final SRMB Co-Chairs ToR Approval dated May 28/2019
- 13 *TB Policy on Government Security (July 1, 2019), Directive on Security Management (July 1, 2019).*
- 14 Departmental Security Plan 2019-22 Version 3.1 February 20, 2019, Section 2.2.3.
- 15 Departmental Security Plan 2019-22 Version 3.1 February 20, 2019, Section 4.4.
- 16 Communications Security Establishment Canada (CSEC) Information Technology Security Guidance – IT Security Management: A Lifecycle Approach (ITSG-33)

- 17 TBS Policy on Government Security.
- 18 Directive on Security Management
- 19 SSC's Policy on Departmental Security
- 20 SSC Directive on Security Management for Enterprise Services
- 21 The Enterprise Business Intake Process through Service Delivery Management provides a centralized approach for customers to make IT business requests. The average cycle time for a Business Request from initial Assessment to Implementation was 173 business days in 2018–19, or approximately 8.25 elapsed months. Upon implementation, the OPI (that is, SMG) triggers billing and Finance invoices the customer once the BR is complete. Including 30 days for settlement, it is estimated, therefore, that cost recovery occurs at least 9.25 months from the start of SA&A activity and, at best, not until the end of the year.
- 22 SA&A Security Standard (Draft), 4.3.3.3 Security Status Reporting
- 23 Risk Aggregation relates to the process of summing and showing the interaction between single or individual risks, to see the bigger picture. According to the Basel Committee's BCBS 239, risk aggregation is defined as the process of defining, gathering and processing risk data.
- 24 PGoF V5 has recently been released to align with the TBS Policy re-set for *Policy on the Planning and Management of Investments* and the *Directive on the Management of Projects and Programmes*
- 25 [This information has been severed]

- 26 [This information has been severed]
- 27 SSC Directive on IT Security Risk Management
- 28 There are three distinct kinds of artifacts in the context of SA&A:
1. Policy/guidance/ standard /process Artifacts: These are corporate or 'best practice' objects used to direct the procedures in use by project and SA&A
 2. Project Artifacts are created BY the system project and **used** by SA&A as input for creating the chain of evidence of security risk mitigation. For example, Project Charter, High Level Diagrams, Concept of Operation (ConOps), etc.
 3. SA&A Artifacts are created **by** SA&A to rationalize / summarize the evidence in security risk mitigation. For example, Final SA&A Plan, Final SRTM and Supporting Documents, Security Assessment Report, etc.
- In the SA&A Audit we are examining the SA&A artifacts (c) and assessing their adequacy.
- 29 Shared Services Canada – Section 8.1.1 Policy on Departmental Security, May 1, 2014
- 30 Shared Services Canada - Section 8.1.2 Policy on Departmental Security, May 1, 2014
-

Date modified:

2020-12-18