Systems under Development Audit of Infrastructure Program Projects

Annual Report 2017-2018

December 18, 2018

Office of Audit and Evaluation

Shared Services Canada
Services partagés Canada
Canada

TABLE OF CONTENTS

EXECUTIVE SUMMARY

What we examined

As part of its efforts to modernize how the federal government manages its information technology infrastructure, Shared Services Canada (SSC) initiated a comprehensive Government of Canada-wide business transformation hinging on six core infrastructure programs. These programs entail greater complexity and magnitude than typical programs, and as such, they were identified and recommended to be reviewed as a suite of system under development (SUD) audits by SSC's Departmental Audit Committee.

To support SSC in managing this complex transformation, the Office of Audit and Evaluation conducted quarterly SUD audit programs of SSC's Information Technology (IT) infrastructure programs in 2016-2017 and 2017-2018.

This report provides a summary of three of the four 2017-2018 SUD audits on the topics of:

- Project Management - Activities vs projects
- Data Centre Consolidation - Data centre closures
- Cyber and IT Security - IT security requirements in procurements

The fourth SUD audit for 2017-2018 on the topic of the Project Management Operating Guide will be published as a separate report.

Why it is important

The success of SSC's Government of Canada (GC) - wide Infrastructure Plan is largely related to the success of the six IT infrastructure programs that are the subject of the SUD audits. These audits contribute to the success of these programs by helping management to assess whether the infrastructure programs are on track and provide an early detection system to identify issues in a timely manner.

What we found

The audit findings focused on areas of highest risk in each of the areas under examination.

Project Management - Activities vs projects: SSC manages a portfolio of activities and projects in the implementation of its Infrastructure Plan. Activities are a series of tasks that can be managed without a rigid oversight process. Projects are more complex and require stricter governance as they produce defined outputs and realize specific outcomes generally in support of public policy objectives.

SSC had established processes and controls for changing activities to projects (and vice-versa) and the impacts of making these changes were understood. There were, however, disparities among the identification, documentation and monitoring of activities. Additionally, criteria to determine the classification of an activity versus a project were not documented or consistently

applied. This resulted in some cases where projects were being managed as activities and activities were being managed as projects.

Activities being managed as projects may be subjected to unnecessary oversight and reporting requirements, while projects being managed as activities may not receive the appropriate funding, resources and oversight. Both situations increase the risk of inefficiencies and ineffectiveness.

In response to these findings, SSC management provided and communicated a formal definition of projects and activities through the Project Governance Framework; revised the project management operating guide and governance process to ensure that decisions and tracking takes place; and will now report regularly to a senior level internal governance committee.

Data Centre Consolidation - Data Centre Closures: This major infrastructure initiative is aimed at closing legacy data centres to provide better service to partners in new enterprise data centres and save money. To do this efficiently and effectively, data centre consolidations need to be prioritized and cost savings from the closures needed to be tracked and reported to senior management.

While some actions were taking place to address the prioritization and execution of data centre consolidations, outstanding issues were still evident regarding incomplete documentation, inefficient data management tools, and reporting to SSC management. The list of planned data centre consolidations was not consistently followed and rationale for changes were not always documented or communicated within SSC or with partners. Changes to the planned consolidations may affect partners and SSC's strategic priorities and goals.

Management committed to improve the deficiencies and management action plans include finalizing a list of planned data centres for consolidation in 2017-2018; ongoing meetings between SSC and key partners to ensure that sites are properly identified for consolidation; developing a communication strategy to engage partners about data centre consolidation plans; and better tracking of data centre consolidation costs and benefits and reporting to senior management.

Cyber and IT Security - IT security requirements in procurements: SSC must ascertain that the processes to identify, assess and approve IT security requirements were established and effectively implemented in procurement processes for infrastructure projects. The audit found that SSC was not always engaging with vendors to ensure security discussions were taking place and had not defined key documentation required to build security requirements. Consultation on security requirements with business owners did not always occur and the roles and responsibilities to approve these requirements were not defined. This resulted in security requirements for some SSC large projects not being well defined or aligned with industry capabilities.

Through the further development of the Project Management and Delivery Operating Guide and the Project Governance Framework, management will address the recommendations. These tools include: the references and linkages to Cyber and IT Security required documentation; and defined roles and responsibilities for developing and approving security requirements.

Next Steps

SSC management is in agreement with the findings from all three audit engagements and has provided management responses and action plans to address the improvements required. At the time of writing of this summary report, over half of the recommendations had been addressed and closed. For details see Annex B.

The Office of Audit and Evaluation will continue to follow up on all outstanding items and provide periodic reporting to SSC's President and Departmental Audit Committee.

Begonia Lojk

Acting Chief Audit and Evaluation Executive

A. INTRODUCTION

1. Background and rationale for the audit

1.1 Background

Shared Services Canada (SSC) was established 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. SSC is delivering mandated email, data centre and network services to partner organizations in a consolidated and standardized manner to support the delivery of Government of Canada (GC) programs and services. With a whole of government approach to IT infrastructure services, SSC is creating economies of scale to deliver more efficient, reliable and secure IT infrastructure services to Government of Canada departments. SSC also provides certain optional technology-related services to government organizations on a cost-recovery basis.

In 2016, the Department conducted a comprehensive reset of its plans to modernize and transform the Government of Canada's information technology systems. The resulting Government of Canada IT Infrastructure Plan outlines SSC's strategic direction, accountabilities and priorities in order to transform the Government of Canada IT infrastructure and improve the digital delivery of programs and services of value to Canadians.

SSC's GC IT Infrastructure Plan relies on the six core SSC infrastructure programs that form the modernization agenda, being:

- Data Centre Consolidation
- Email Transformation Initiative
- Workplace Technology Devices
- Cyber and Information Technology Security Transformation
- Telecommunications Transformation Program
- IT Service Management Transformation

These six major infrastructure programs are recognized as being highly complex, significant in cost and critical to the success of the GC's overall modernization agenda. Each of the infrastructure programs encompass numerous projects, with continued evolution and rapid development to achieve stated targets, with particular focus on GC-wide annual savings and improved efficiency.

To support SSC in managing the complex transformation of the IT infrastructure, the Office of Audit and Evaluation began conducting quarterly System under Development (SUD) audits of SSC's infrastructure programs in 2016-2017. To date, eight SUD audit programs have been completed, with two more in progress. The first four quarterly SUD audits, summarized in the 2016-2017 SUD annual report, covered the following subjects:

- Transformation planning

- Performance reporting and financial management
- Government of Canada Wide Area Network project
- Workload migrations

This report summarizes the first three SUD audit programs that were performed in 2017-2018:

- Project Management - Activities vs projects
- Data Centre Consolidation - Data centre closures
- Cyber and IT Security - IT security requirements in procurements

In 2017-2018 a decision was taken to finalize each SUD audit program in a separate standalone audit report. As a result the final 2017-2018 SUD audit on the topic of Project Management will be published as a separate audit report.

1.2 Rationale for the audits

The success of SSC's GC-wide Infrastructure Plan is dependent on the success of the six IT infrastructure programs that are the subject of the SUD audits. As such, the SUD audits contribute to the success of these programs by helping management to assess whether the infrastructure programs are on track and provide an early detection system to identify issues in a timely manner.

The topics selected for 2017-2018 were done so on a risk basis.

1.3 Audit Authority

The Audit was included in the 2017-2020 Risk-Based Audit Plan, which was approved by the President of Shared Services Canada following the recommendation of the Departmental Audit Committee.

2. Objective, scope and methodology

2.1 Objective

The overall objectives of the SUD audits are to provide management with an assessment of:

- The progress and attainment of each program's objectives at defined milestones within the program and across the transformation agenda.
- Key internal controls, governance processes and transformation risk management framework at a point in the development cycle where enhancements can be implemented and processes adapted.

Each quarterly SUD audit program has its own unique focus and set of objectives and audit criteria. In this report the objectives of the three topics covered were the following:

- **Project Management - Activities vs Projects**: To determine if the processes and controls to change transformation projects to activities (and vice-versa) were established, adhered to, and that the implications of the changes were understood.
- **Data Centre Consolidation - Data Centre Closures**: To determine whether data centre consolidations were prioritized and executed effectively and also to determine if cost savings from data centre consolidations were tracked and accurately reported.
- **Cyber and IT Security - IT Security Requirements in Procurements**: To ascertain that the processes to identify, assess and approve IT security requirements were established and effectively implemented.

2.2 Scope

The scope was limited to processes and controls within SSC's IT Infrastructure Programs: Email Transformation Initiative, Workplace Technology Devices, Telecommunications Transformation Program, Data Centre Consolidation and Cyber and Information Technology Security, and IT Service Management.

2.3 Methodology

The SUD audit approach incorporates the following key characteristics:

- Top-down, risk-based approach with an integrated perspective across infrastructure programs that accounts for program interdependencies.
- Continued planning, execution, reporting and planning refinement for each quarterly cycle to enforce continued alignment between SUD audit resource allocation and risks/priorities to SSC.

The SUD audit assesses (qualitatively and quantitatively) whether the programs are on track, identifying key issues in a timely manner.

During the execution phases of the audits the following procedures were conducted:

- Interviewed SSC senior managers, managers and personnel.
- Reviewed relevant documents, such as previous audits, government guides and policies with regard to project management, and SSC project management process documentation.
- Performed data analysis.

The first SUD audits were conducted on a cyclical basis and are rolled up into an annual report. The fifth, sixth and seventh SUD audits, completed in 2017-2018, are summarized in this annual report. New SUD audits will be presented individually in separate reports as they are completed.

2.4 Statement of Conformance

The audit conforms to the International Standards for the Professional Practice of Internal Auditing as supported by the results of the quality assurance and improvement program. A practice inspection has been passed.

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. The findings and conclusion are only applicable to the entity examined and for the scope and time period covered by the audit.

B. SUMMARY OF FINDINGS

1. Project Management - Activities vs. Projects

1.1 Background

Sound and effective project management is essential to support SSC's infrastructure programs. In 2017 the Project Management and Delivery Branch was created to provide centralized project management processes, sound governance and effective project management oversight. It was important to review early how effectively the new project management processes have been set up in order to provide feedback to SSC management.

The distinction between activities and projects is a critical concept in sound project management. It is essential to ensure that both are appropriately managed to ensure proper governance and efficient management practices.

In general, activities are series of tasks that do not require a rigid governance process. While projects are required to produce defined outputs and realize specific outcomes in support of a public policy objective; they require a clear schedule, resource plan and governance process. Activities that are incorrectly managed as projects may be subjected to unnecessary governance and reporting requirements. Projects that are managed incorrectly as activities may not receive the appropriate funding, resources and oversight. Both situations increase the risk of inefficiencies and ineffectiveness.

1.2 About the Audit Program

This audit focused on processes and controls related to change processes for transformation activities and projects. This is important because any deficiencies in these processes and control elements could have an impact on projects receiving appropriate funding, resources and oversight; therefore affecting their overall effectiveness and efficiency.

The objective was to determine if the processes and controls to change activities to projects (and vice-versa) are established, being adhered to and to understand the implications of these changes. The scope included IT infrastructure projects that were changed from activities to projects (and vice-versa) from the period of January 1, 2016 to December 31, 2016. The examination phase was conducted from January 8, 2017 to March 16, 2017.

1.3 Findings

Inconsistencies were found in the thresholds applied to determine the classification of an activity vs a project; these were not documented or consistently applied at the time of the audit. Even though SSC had adopted Treasury Board of Canada's project definition, this definition had not been applied to the unique transformational and operational nature of the department. This led to inconsistencies in interpretation and application across branches. In response to this finding, SSC

management provided and communicated a formal definition of projects and activities through the Project Governance Framework.

The audit found that SSC systems adequately tracks projects and services, but does not track activities to the same extent. For example, a process did not exist to accurately categorize activities or identify and correct errors in categorization for activities. An inventory of activities that support the GC IT Infrastructure Plan did not exist, and there were no systematic processes for tracking and monitoring these activities. Without these processes in place there is a risk that activities will be inaccurately reported and interdependencies among projects and activities can be missed. SSC management is in agreement with this finding and revised the project management operating guide and governance process to ensure that decisions and tracking takes place.

IT infrastructure projects identified in the project record management system were not consistent with those identified in the GC IT Infrastructure Plan. SSC will not be able to accurately report on progress against the Plan unless projects are consistently identified and tracked. SSC management will now report regularly to a senior level internal governance committee.

2. Data Centre Consolidation - Data Centre Closures

2.1 Background

SSC manages over 500 aging legacy data centres that support mission-critical and non-mission-critical business functions for the 43 departments and agencies that are part of SSC's mandate. The most cost-effective way to address the government's "rust out" issue is to consolidate these data centres into fewer modern and secure data centre services. Data centre consolidation is a key element of SSC's infrastructure plan that culminates with the closure and decommissioning of the aging legacy data centres.

It is important for SSC to have a clear and prioritized plan by which it will be able to meet its data centre consolidation commitments. It is also necessary to have accurate information on costs in order to understand the financial benefits that will accrue with the timely closures and decommissioning of legacy data centres.

2.2 About the Audit Program

This audit focused on the management and oversight of the data centre closure process. Strong governance processes would ensure the Department's ability to accurately report against its data centre consolidation commitments and to track program cost.

This subject is important because changes to data centre closure priorities can affect SSC's ability to meet its planned consolidation objectives and partners' business plans and funding commitments. Accurate tracking of costs and benefits will help SSC report on the accrued benefits of data centre consolidation.

The audit objectives were to determine whether Data Centre closures are prioritized and executed effectively; and to determine if cost savings from data centre closures are tracked and are being accurately reported. The scope included relevant processes and controls for data centre closures and realizing cost savings within SSC. The examination phase for this audit began on April 20, 2017 and was completed on June 9, 2017.

2.3 Findings

The audit found that while some activities were taking place to address the prioritization of data centre closures, issues regarding incomplete documentation and inefficient data management tools resulted in an inability to track and reconcile costs in a comprehensive manner.

For example, at the time of the audit, SSC's list of data centres identified for closure was not accurate nor up-to-date. Management was aware of this and had already begun work to review the listing. SSC will also implement a process to ensure its completeness.

In the sample reviewed, the artefacts kept on the various data centres in the SSC tracking tool did not contain all required information on data centres and their associated costs. Also the process to collect and validate the information received was not performed consistently. Much of

the information was populated when SSC was initially created and management now needs to put in place a process to update and keep the information accurate.

Data centre closure plans in 2016-2017 were not carried out as scheduled. Only about one-third of planned data centres closures were completed and four data centres not on the original plan were closed. The rationale for these changes was not always documented or communicated within SSC or with partners. While deviations from the plan will always be necessary due to natural disaster and failing infrastructure, it remains important to prioritize data centre closures in an approved plan and to clearly communicate this plan to partners and stakeholders. SSC management is working on a prioritization strategy and plan,

Costs and benefits accruing from data centre closures were not accurately tracked and reconciled to the financial systems. This means that costs and savings cannot be analysed and accurately reported, and that proper planning and prioritization will be challenging. Management has agreed to improve its cost tracking.

3. Cyber and IT Security - IT Security Requirements in Procurements

3.1 Background

Procurement processes are a key enabler for many of SSC's infrastructure projects. It is important that SSC's procurement processes are designed to include IT security requirements. This will help to ultimately achieve effective IT security practices in SSC's infrastructure projects.

In order to ensure successful procurement processes, it is necessary to collaborate with stakeholders such as vendors to ensure alignment with industry norms and the overall feasibility of the procurement request. Limited consultation with partners and stakeholders may lead SSC to provide security profiles that are overly prescriptive, add unnecessary costs and delays to projects, or are not aligned with industry capabilities.

At the start of a procurement process, security requirement criteria must be clearly documented in request for proposal documentation and appropriately approved. It is important that relevant input is obtained to ensure that security requirements are aligned to business needs of the service lines.

3.2 About the Audit Program

This audit focused on assessing SSC's IT security requirement process controls and their implementation in procurement vehicles. Issues with these controls or their implementation could result in SSC's IT-projects not being aligned with industry standards or not meeting security requirements. Without proper approval from the appropriate authority there is a risk that incorrect security requirements may affect the overall project and security of the infrastructure

The objective was to ascertain that the processes to identify, assess and approve IT security requirements in procurement are established and effectively implemented. The scope included relevant processes and controls pertaining to the identification, assessment and approval of security requirements for projects as they are provisioned for procurement. A sample of three major infrastructure program projects was selected to identify whether the correct processes were followed for identifying, assessing and approving the security requirements included in Request for Proposals. The examination phase was conducted from July 4, 2017 to September 15, 2017.

3.3 Findings

The audit reviewed the extent to which vendors were engaged on the feasibility of the defined security requirements in the review and refine requirements phase of three large procurements. In one case there was no engagement with vendors and subsequently the procurement failed. In the two cases where the vendors were engaged, not all of the vendors' questions were fully answered by SSC. SSC's management has agreed to revise the procurement process in order to ensure that collaboration occurs, exceptions are appropriately approved and that all vendor questions are appropriately addressed.

The audit noted that documentation needed by the Cyber and IT Security Branch to identify security requirements was not consistently defined. Also key security discussions were not always taking place with the service lines. As a result, necessary documents were not consistently provided by the project teams in support of security requirements, increasing the risk of error and inadequate security requirements. SSC management will develop and communicate a process to ensure that security information is collected and service line consultation is undertaken, as part of SSC's project governance framework.

Finally, the audit found that the authority to approve the final security requirements included in request for proposals was not defined. In the sample reviewed there was no evidence of approval of security requirements by the Cyber and IT Security Branch. Management will define and communicate roles and responsibilities for this approval.

C. CONCLUSION

In this annual cycle of SUD audits, the Office of Audit and Evaluation conducted four quarterly audits. Three of these are summarized in this report; they are focussed on: infrastructure activities vs. projects; data centre closures, and IT security requirements in procurements. These audits were important as they touched on key business processes that supported SSC's infrastructure plan.

The overall results of the three SUD audits included in this report demonstrate that while SSC continues to deliver on its infrastructure plan and program objectives, there are inconsistencies in terms of the establishment and adherence to firm processes and governance structures. With the Department continuing to move forward in meeting the first audit objective (i.e. attainment of project objectives), more work is required to advance toward meeting the second audit objective (refinement and adaptation of key internal controls, governance processes and transformation risk management framework).

Since the completion of these audits, management has produced management action plans to address the risks that were identified (see Annex B). SSC's Office of Audit and Evaluation is monitoring the implementation of these action plans. At the time of publication of this report, over half of the action plans had been completed and SSC is committed to implementing the remaining ones.

ANNEX A: SUD AUDIT PROGRAM SCHEDULE

Title	Period of Conduct
SUD 1: Transformation Planning	January to March 2016
SUD 2: Performance Reporting and Financial Management	April to June 2016
SUD 3: Telecommunications Transformation Program: GC Wide Area Network	July to September 2016
SUD 4: Data Centre Consolidation: Workload Migrations	October to December 2016
SUD 5: Activities vs. Projects	January to March, 2017
SUD 6: Data Centre Closures	April to June, 2017
SUD 7: IT Security Requirements	July to September, 2017
SUD 8: Project Management Operating Guide	October to December 2017
SUD 9: High Performance Computing	March to April 2018
SUD 10: Project Cost Management	June to September 2018

ANNEX B: RECOMMENDATIONS AND MANAGEMENT RESPONSES

The following table includes the recommendations included in each of the System under Development Audit, along with management response.

Status of management action plans for each recommendation as of September 2018 are indicated below.

SUD 5: Activities vs Projects

Recommendations:

5.1 We recommend that the Senior Assistant Deputy Minister Project Management and Delivery develop, approve and communicate service defined thresholds that support the accurate classification of projects and activities. **Completed**

5.2 We recommend that the Senior Assistant Deputy Minister Project Management and Delivery update and clarify the process for changing transformation activities to transformation projects (or vice versa), as required. **Completed**

5.3 We recommend that the Senior Assistant Deputy Minister Project Management and Delivery identify [Retracted by ATIP] and ensure the list is updated and used consistently throughout SSC. **Completed**

SUD 5 Activities vs Projects Management Response:

Management agrees with these recommendations and has developed action plans to address the risks identified by the audit. In these action plans, management committed to the formal establishment and communication of clearly defined service levels in support of comprehensive project and activity classification. To this end, management will clearly update the processes for changing transformation activities to processes (or vice versa), as well as clearly *[Retracted by ATIP]* and keeping it current and effective as a tool for regular use.

SUD 5 Activities vs Projects Management Update December 2018:

Project Management & Delivery Branch has developed and published the Project Management and Delivery Operation Guide which:

- Provides a reference tool for SSC specific processes, following industry best practices in accordance with the Project Management Institute's Project Management Body of Knowledge (PMBoK) and the Treasury Board Policy on the Management of Projects.
- Provides a guideline in determining whether an initiative is either a project or an operational activity.
- Strengthens and better defines the relationship between Transformation Planning Process and Project Governance Process.

A project list was approved through SSC Governance and is maintained, updated and used on a regular basis.

SUD 6: Data Centre Closures

Recommendations

6.1.1 We recommend that the Assistant Deputy Minister, Data Centre Services:

- Develop and document a process that accurately prioritizes data centres as high, medium and low priority (accounting for emergency closures) and updates approved plans and the closure list based on management priorities, funding and capacity; and
- Establish and communicate a process to approve deviations/exceptions from the data centre prioritization, including documentation of impacts (on scope, timelines, budget and monetization).
- **In progress**

6.1.2 We recommend that the Assistant Deputy Minister, Data Centre Services:

- Conduct a reconciliation of all data centre lists to ensure that the final list is complete and accurate for planning and prioritization; and
- Conduct periodic validation exercises to ensure that the official data centre closure list is kept up to date.
- **In progress**

6.1.3 We recommend that the Assistant Deputy Minister, Data Centre Services:

- Identify key information that factors into Data Centre Closure prioritization and benefits realization1 within the Data Centre Closure Application tool (including mandatory artefacts for the end to end data centre closure processes).
- Communicate requirements for any data collection tools and clearly indicate mandatory data fields to collect key information and ensure completeness.
- Document evidence of site visits, approvals and validation of data collected to ensure information accuracy.
- **In progress**

6.2.1a We recommend that the Assistant Deputy Minister, Data Centre Services:

- Document a data centre closure plan, in collaboration with partners, which should include roles and responsibilities, timelines, resourcing requirements and sign-offs from relevant partners; and
- Complete and obtain Letters of Agreement to transfer space and/or monetization from all partners for closures to be completed in the given fiscal year.
- **In progress**

6.2.1b We recommend that the Senior Assistant Deputy, Project Management and Delivery Branch ensure unfunded/discontinued projects are removed for active project status reports. **Completed**

6.3.1a We recommend that the Assistant Deputy Minister, Data Centre Services ensure cost estimates for Data Centre Closure contained in the Data Centre Closure Application tool are corroborated by appropriate supporting documentation. **In progress**

6.3.1b We recommend that the Assistant Deputy Minister, Chief Financial Officer:

- Ensure that individual data centre closure costs and monetization received can be tracked and reported in a timely manner to senior management; and
- Collaborate with Data Centre Services to reconcile costs and benefits of Data Centre Closures from the Data Centre Closure Application tool to Sigma.[2]
- **In progress**

[1] This information may include, but is not limited to occupancy instrument expiry, lease expiry, monetization, space measurements, emergency issues, etc.
[2] Sigma is a key financial system used by SSC for the tracking and monitoring of costs and benefits associated with activities, projects and programs.

SUD 6 Data Centre Closures Management Response:

Management agrees with these recommendations and has developed action plans to address the risks identified by the audit. In these action plans, management committed to leveraging available tools and information to ensure the data centres list was complete, accurate and subject to regular validation with the goal of engaging in prioritized, up-to-date closure activity that is and communicated accordingly. Management also committed to further planning and collaboration with partners to better coordinate closure and financial activity.

SUD 6 Data Centre Closures Management Update December 2018

The Data Centre Services Branch has addressed the audit findings through various management action plans developed against 5 recommendations where Facilities Management has been leading the work being done on behalf of the branch. Tracking and prioritization tools, communications and partner engagement strategies, funding requirements and expenditure tracking, process and data validation tools and other activities have been presented in a comprehensive Data Centre Closures Playbook. The documentation and processes were discussed, drafted and finalized as part of a two-part workshop having taken place on June 28th, 2018 and October 10th, 2018. The working group consisted of key stakeholders including partner departments and other implicated SSC branches.

The first release of the Data Centre Closures Playbook was completed and is in the process of general distribution. Included, are a number of processes to ensure improved data integrity and proper communication practices. Data Centres Services Branch management action plans were completed and submitted as part of Departmental Audit Committee management action plan follow-up exercises leading up to the February 2018 Departmental Audit Committee meeting.

The Project Management and Delivery Branch is ensuring the active project list is kept up to date and unfunded/discontinued projects are removed from the active project status reports on a regular basis.

The Chief Financial Officer Branch has established a process so that data centre closure costs can be tracked in SIGMA by site closure. Internal Order codes were created in order to be able to track the costs per closure. In addition, the monetization benefits are labeled in the initial budget allocation and in subsequent supplementary estimates and can be reported to senior management in a timely manner.

SUD 7: IT Security Requirements in Procurements

Recommendations:

7.1.1 We recommend the Senior Assistant Deputy Minister Corporate Services implement controls to ensure that all vendor inquiries are responded to during the Review and Refine Requirements (RRR) process. **Completed**

7.1.2 We recommend the Senior Assistant Deputy Minister Corporate Services update the Directive on Procurement Governance to ensure that the decision to forego and phase of the collaborative procurement process be referred to the highest level of Governance of a given procurement as defined in the Directive on Project Governance. **In progress**

7.2.1 We recommend that Assistant Deputy Minister Cyber and IT Security develop and communicate a process that requires documented input from the project teams to support the creation of the security requirements (including privacy impact assessments) that are being included in the Request for Proposal. **Completed**

7.2.2 We recommend that Senior Assistant Deputy Minister Project Management and Delivery include required documentation (as determined by Cyber and IT Security) within the Project Management and Delivery Operating Guide and/or the Project Governance Framework. **Completed**

7.3.1 We recommend that Assistant Deputy Minister Cyber and IT Security, in consultation with the Senior Assistant Deputy Minister Project Manager and Delivery, confirm and communicate the roles and responsibilities for developing and approving the final security requirements to be included in Request for Proposals. **Completed**

7.3.2 We recommend that Senior Assistant Deputy Minister Project Management and Delivery include roles and responsibilities for developing and approving security requirements for projects within the Project Management and Delivery Operating Guide. **Completed**

SUD 7: IT Security Requirements in Procurements Management Response:

Management agrees with these recommendations and has developed action plans to address the risks identified by the audit. In these action plans, management committed to improving the Department's relationships with vendors through better controls around the initial procurement processes and a stronger review and approval function for more complex projects. Concerning Requests for Proposals, management committed to creating a robust security clearance requirement process and ensuring that essential documentation is provided within its guides and frameworks. Roles and responsibilities pertaining to the development and approval of security requirements are to be confirmed and clearly stated within request for proposals and operational guides.

SUD 7: IT Security Requirements in Procurements Management Update December 2018:

The Cyber and Information Technology Security Branch has developed the Security Assessment Plan template to document the process by which all new or updated systems will be assessed for security risks prior to implementation on SSC's Infrastructure. The Security Assessment Plan template:

- requires documented input from project teams;
- supports the creation of security requirements;
- defines security requirements roles and responsibilities and
- must be completed for every project impacting the IT infrastructure operated by SSC.

To date, the Security Assessment Plan template is being used to document and report on the security assessment process and results for all IT projects impacting SSC's infrastructure.

The Project Management and Delivery Branch has updated the Project Management and Delivery Operating Guide with a live link which provides access to the Cyber and IT Security requirements, including inputs necessary for the development of project security requirements. The updated Project Management and Delivery Operating Guide also outlines the roles and responsibilities for developing and approving security requirements for projects based on the input from the Cyber and IT Security Branch.

The Corporate Services Branch has undertaken a comprehensive review of procurement governance to identify opportunities to streamline oversight and clarify accountabilities. A revised Procurement Governance Framework will be approved by June 20, 2019.

ANNEX C: ACRONYMS

Acronym	Name in Full
GC	Government of Canada
IT	Information Technology
SSC	Shared Services Canada
SUD	System under Development