TREASURY BOARD OF CANADA SECRETARIAT DETAILED ACTION PLAN

to the recommendations of the Independent Auditors Report of Cybersecurity of Personal Information in the Cloud

Report Ref. No.	OAG Recommendation	Departmental Response	Description of Final Expected Outcome/Result	Expected Final Completion Date	Key Interim Milestones (Description/Dates)	Responsible Organization/ Point of Contact (Name, Position, Tel #)	*Indicator of Achievement* (For Committee Use Only)
33	In consultation with Shared Services Canada and Public Services and Procurement Canada, Treasury Board of Canada Secretariat (TBS) should: • Clarify who is responsible for validating and ongoing monitoring of cloud guardrails controls on an ongoing basis, and clarify the processes to be followed. • Extend the requirement for guardrails to cloud service provider contracts stemming from supply arrangements established by Public Services and Procurement Canada.	TBS will clarify the process & roles/responsibilities for validating and monitoring of guardrails & extend to PSPC procured solutions.	Published Cloud Responsibility Matrix, that formally identifies who is responsible for validating, ongoing monitoring, performing oversight and compliance of the cloud guardrails controls. The Standard Operating Procedure for Validating Cloud Guardrails is clarified and extended for cloud service provider contracts awarded by PSPC. The GC Cloud Guardrails and Directive on Service and Digital is updated to reflect guardrail controls that apply to cloud services including PSPC procured cloud services. In addition, TBS will: • establish a score card to report on departments' level of adherence to the GC Cloud Guardrails, • collaborate with SSC in their efforts to implement tools to automate guardrail monitoring for cloud service providers in the Government of Canada; and • continue to provide advice and guidance to departments on ensuring that they perform security assessment and authorization activities for cloud-based applications using tools such as the Security Playbook for Information System Solutions which outlines a set of security tasks for consideration when designing and implementing solutions for Government of Canada (GC) information systems in cloud environments.	April 1, 2023	October 6, 2022 - publish the Cloud Responsibility Matrix December 2022 - clarify applicable guardrails for PSPC procured solutions and extend to PSPC procurement. January 2023 - update the guardrails, including PSPC February 2023 - establish a score card report template April 2023 - collaboration with SSC on automation of guardrails reporting proof of concept complete and onboarding of departments begins.	Scott Levac, Director – Cloud Oversight, 613-793-7207 Rahim Charania, Director - Cyber Security, 613-612-7808	
42	TBS should ensure that: • The Government of Canada Cyber Security Event Management Plan is relevant to the evolving cloud environment and shared responsibilities, is reviewed and tested annually, and updated if changes are warranted. • Departments finalize, implement, and regularly test their security event management plans.	TBS will ensure relevance of the GC Cyber Security Event Management Plan (GC CSEMP) and that it is reviewed and tested annually and updated if required. Ensure departments use GC CSEMP.	The Government of Canada Cyber Security Event Management Plan will be reviewed and tested at least annually and updated as appropriate. This includes an update to the GC CSEMP and inclusion of cloud-based scenarios in GC CSEMP simulation exercises; A process will be in place to validate that Departments have established and implemented a Departmental CSEMP that aligns with the GC CSEMP, that are submitted on an annual basis to TBS for review. Tools are planned for and available which will enable departments to regularly test their Departmental CSEMP, such as a canned tabletop product that focuses on a cloud-based scenario that departments can leverage to run their own simulation exercise; as well as exploring		Fall 2022 - GC CSEMP updated and published March 2023 – Explore options for tools to enable departments to facilitate cloud-based simulation exercises April 2023 – Include a requirement for departments to submit their CSEMP with their Plan for Service and Digital	Rahim Charania, Director - Cyber Security, 613-612-7808	

Report Ref. No.	OAG Recommendation	Departmental Response	Description of Final Expected Outcome/Result	Expected Final Completion Date	Key Interim Milestones (Description/Dates)	Responsible Organization/ Point of Contact (Name, Position, Tel #)	*Indicator of Achievement* (For Committee Use Only)
			options to establish a procurement vehicle that will enable facilitated cloud-based simulation exercises by March 2023.				
51	In consultation with Communications Security Establishment Canada, Shared Services Canada, Public Services and Procurement Canada, and departments, Treasury Board of Canada Secretariat should ensure that roles and responsibilities required in support of the design, implementation, validation, monitoring, coordination and enforcement of all the security controls needed to protect sensitive and personal information in the cloud are documented and proactively communicated to any department that is using or considering the use of cloud services. These documented roles and responsibilities would facilitate a complete and common understanding of each department's roles and responsibilities and would facilitate coordination between all departments. The secretariat should review and update these documented roles and responsibilities at least every 12 months.	TBS will ensure that roles and responsibilities required for security controls are clearly documented and proactively communicated to departments. Review and update annually.	Published Cloud Responsibility Matrix, that formally identifies who is responsible for validating, ongoing monitoring, performing oversight and compliance of the cloud guardrails controls. The Cloud Responsibility Matrix is updated following a completed review that has examined and updated the roles and responsibilities required in support of the design, implementation, validation, monitoring, coordination and enforcement of all the security controls needed to protect sensitive and personal information in the cloud. Regular update engagements are arranged for GC Enterprise Architecture Review Board, Director General Cloud Steering Committee, GC Cloud and Computing Network of Expertise Working Group to proactively share information on roles and responsibilities to any department that is using or considering the use of cloud services. Updates to the Cloud Responsibility Matrix are published to information sharing sites such as the GC Cloud InfoCentre. A process is established for an annual review and publication of the Cloud Responsibility Matrix and providing updates to the community.		October 6, 2022 - publish the Cloud Responsibility Matrix March 2023 - complete a review of the responsibility matrix September 2023 - increase proactive communications March 2023 - updates to the community on review cycles	Scott Levac, Director – Cloud Oversight, 613-793-7207 Rahim Charania, Director - Cyber Security, 613-612-7808	
62	Treasury Board of Canada Secretariat, in consultation with Shared Services Canada and other departments, should: • Develop and provide a costing model to help departments make informed decisions about moving to	TBS will develop and provide a costing model and tools to help departments make informed decisions about moving to the cloud and determine resources and funding required.	Completed TBS consultations with the GC community to discuss cloud operational models, prioritization criteria and associated funding models. A series of recommendations presented to the GC CIO on direction for operating in the Cloud.		Fall 2022 – Recommendations to GC CIO on path forward June 2023 - provide a costing model & guidance	Scott Levac, Director – Cloud Oversight, 613-793-7207	

Report Ref. No.	OAG Recommendation	Departmental Response	Description of Final Expected Outcome/Result	Expected Final Completion Date	Key Interim Milestones (Description/Dates)	Responsible Organization/ Point of Contact (Name, Position, Tel #)	*Indicator of Achievement* (For Committee Use Only)
	the cloud, and determine whether additional resources and funding are required. • Help departments determine their operational funding needs and sustain their funding so they can fulfill their evolving responsibilities for cloud operations, including securing sensitive information in the cloud.		TBS Consultations with SSC and departments complete. Outcomes include a costing model and guidance to help departments make informed decisions about moving to the cloud. Tools and guidance available intended to assist departments, including SSC, with forecasting medium and long term costs required to operate in a cloud environment.		June 2023 - assist departments & SSC with forecasting		