Communications Security Establishment
Centre de la sécurité des télécommunications

UNCLASSIFIED

MANAGEMENT SERIES

INFORMATION TECHNOLOGY SECURITY GUIDANCE

CLOUD SERVICE PROVIDER INFORMATION TECHNOLOGY SECURITY ASSESSMENT PROCESS

ITSM.50.100
August 2018

Canada

FOREWORD

This description of the Cloud Service Provider (CSP) Information Technology Security (ITS) Assessment Process is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at CSE.

For further information, please contact CSE's ITS Client Services area by e-mail at ITSclientservices@cse-cst.gc.ca, or call 613-991-7654.

EFFECTIVE DATE

This publication takes effect on 31 August 2018.

OVERVIEW

The purpose of this document is to describe CSE's Cloud Service Provider (CSP) Information Technology Security (ITS) Assessment Program. The objective of the CSP ITS Assessment Program is to assist Government of Canada (GC) departments and agencies in their evaluation of CSP services being procured for use by the GC. The resulting assessments will show whether the subject CSP's security processes and controls meet the GC public cloud security requirements for information and services up to Protected B, Medium Integrity, and Medium Availability (PB/M/M) as published by the Treasury Board of Canada Secretariat [2].

The purpose of this program is to determine if the requirements of the GC-selected security controls and enhancements as outlined in *ITSG-33 IT Security Risk Management: A Lifecycle Approach, Annex 3 – Security Control Catalogue* [1] are satisfied to an acceptable level of assurance. These assessments may be completed using existing guidance, standards, and reports from the GC and allied agencies, industry best practices, and commercial attestations. This will allow for faster evaluations and encourage CSPs to work with the GC, external third-party auditors, and other assessment agencies. The desired end state for the GC is to have a clear understanding of the ITS capabilities and residual risks for the cloud service being used by the GC.

The advice and guidance provided as a result of these ITS assessments are to help GC departments with their risk management decisions when procuring a public cloud service.

Departments procuring public cloud services should ask the following questions:

- Are the risks identified in the resulting reports acceptable?
- Are there security measures that could be implemented to mitigate the identified deficiencies?
- Should we choose a different service?

TABLE OF CONTENTS

1 INTRODUCTION

The purpose of this document is to describe CSE's CSP ITS Assessment Program. The objective of this program is to help GC departments and agencies evaluate CSP services being procured for use by the GC. The resulting assessments will show whether the security processes and controls of the CSP being considered meet the GC public cloud security requirements for information and services up to Protected B, Medium Integrity, and Medium Availability (PB/M/M), as published by TBS [2].

This program will determine if the requirements of the GC-selected *ITSG-33* security controls and enhancements are satisfied with an acceptable level of assurance. The assessments may be done using existing guidance, standards, reports from the GC and allied agencies, industry best practices, and commercial attestations[1]. This will allow for faster evaluations and will encourage CSPs to work with the GC, external third-party auditors, and other assessment agencies. The goal for the GC is to have a clear understanding of the ITS capabilities and residual risks for the cloud service being used by the GC.

The advice and guidance from these ITS assessments are to help GC departments with their risk management decisions when procuring a public cloud service. Departments procuring public cloud services should decide if the risks identified in the reports are acceptable, if there are mitigating security measures that could be implemented to compensate for the identified deficiencies, or if a different service should be chosen.

A detailed knowledge of many security domains is required to completely understand the security posture of any information technology system. Likewise, areas that must be examined to fully understand a CSP's security capabilities and deficiencies include ITS, the physical security of the CSP's data centres, the personnel security of its privileged users, its adherence to Canadian privacy regulations, as well as other areas. CSE's role in this process is to provide advice and guidance on the CSP's technical, operational, and procedural ITS capabilities. Departments who are considering using cloud services will also need to evaluate all security requirements identified in TBS's *Operational Security Standard: Management of Information Technology Security* (MITS) [4] and other relevant GC regulations and policies.

[1] This document uses the term *attestation* generically to mean any ITS-related certification or assessment to which CSPs may subject their services. These include, for example, Service Organization Control 2 (SOC2) and International Electrotechnical Commission / International Organization for Standardization (IEC/ISO) 27001 standard.

PURPOSE

This document describes the process CSE will use to determine the ITS capabilities and residual risks for public cloud services being used to support GC PB/M/M services and information.

CONTEXT

These assessments will only consider the confidentiality, integrity, and availability requirements for GC IT services and information. They will not consider data residency requirements as defined in the TBS *Policy on Management of Information Technology* [3].

The IT risk management process described by TBS in the *GC Cloud Security Risk Management Approach and Procedures* [5] includes the following nine activities:

- Performing the security categorization (in terms of confidentiality, integrity, and availability) of each GC service being deployed on a cloud service
- Selecting an appropriate set of security controls based on the GC service's security category
- Selecting the right cloud deployment model and cloud service model for the GC service
- Assessing the implementation of the security controls in the supporting cloud service
- Implementing the required security controls in the GC service
- Assessing the implementation of these security controls in the GC service
- Authorizing operations of the resulting cloud-based GC service
- Continuously monitoring the security of the cloud-based GC service during the operational phase
- Maintaining the authorization state of the cloud-based GC service

The approach and procedures described in this document are intended to support GC departments and agencies procuring public cloud services when completing the fourth step (above) of the cloud security risk management process: "Assess the implementation of the security controls in the supporting cloud service." The security posture and residual risk of the GC information and services in the CSP will depend on the GC effectively completing the remaining cloud security risk management activities.

TARGET AUDIENCE

The assessments produced following this process are specific to the business-requirement and risk-acceptance scenarios as described above. It is important that the department or agency using these assessments, as part of their cloud security risk management process, ensure their security categorization and information security requirements are consistent with those used for developing the TBS cloud security profiles.

DEFINITIONS

The cloud computing definitions as found in The National Institute of Standards and Technology *(NIST) Special Publication 800-145, The NIST Definition of Cloud Computing* [5] will be used throughout this document. A glossary of terms can be found at the end of this document.

2 ASSESSMENT PROCESS

2.1 OVERVIEW

Conducting comprehensive and independent ITS assessments of CSPs requires time and extensive financial and personnel resources. Fortunately, most CSPs get and maintain internationally-recognized ITS attestations to provide their services to certain industry segments and governments. Some of these attestation programs include the United States Federal Risk and Authorization Management Program (FedRAMP), the American Institute of Certified Public Accountants (AICPA) Service Organization Controls (SOC), and International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) standards. Independent third parties verify compliance with these attestation standards which allows CSPs to satisfy most of their client base's security requirements. CSPs can make their attestations reports available to show compliance and provide assurance in the security posture of their cloud services.

The CSE CSP ITS assessment process uses evidence from these and other third-party assessed attestations wherever possible. When sufficient assurance of compliance with required GC IT security controls and enhancements cannot be obtained from existing attestations, additional evidence is requested from the CSP. If evidence cannot be provided, or if it is determined that the CSP does not meet the requirements of GC IT security controls or enhancements, mitigation measures or risk acceptance will be recommended.

2.2 SCOPE

These assessments will be limited to the following areas of consideration:

- Public CSP services available to GC clients
- GC confidentiality, integrity, and availability requirements as defined in the TBS Cloud Security Profile [2] for PB/M/M or below
- Security measures that have been identified by the CSP as necessary for CSP clients to implement and manage to meet GC PB/M/M ITS security requirements

The following areas will be excluded from these assessments:

- Verification that the CSP data centres in Canada meet GC physical security requirements
- Verification that personnel employed by the CSPs to support services in Canada have been screened to meet GC personnel security requirements or have achieved accepted equivalencies
- GC privacy requirements except for the protection of confidentiality, integrity, and availability of GC information
- Canadian data residency requirements

2.3 REVIEW PARAMETERS

The CSE CSP ITS assessments will be based on a comparison of the *TBS Cloud Security Profile* [2] against international and industry attestations which have been evaluated by third-party assessors that are acceptable to the GC. The details of each IT security requirement are defined in the *ITSG-33 Annex 3 – Security Control Catalogue* [1].

At this time, only the following attestation standards have been compared with the *ITSG-33* control and enhancement requirements:

- System Security Plans (SSP) produced for FedRAMP
- AICPA SOC 2 Type II reports
- ISO/IEC 27001 reports
- ISO/IEC 27018 reports

As the CSE CSP security assessments and the CSP ITS assessment program mature, additional attestation standards will be compared to the *ITSG-33* control and enhancement requirements. The aim is to set up a knowledge base of all attestations commonly held by CSPs. That knowledge base will be used to confirm that the CSPs comply with GC ITS security and assurance requirements.

2.4 ASSUMPTION

Independent third-party auditors will verify that the information in the attestations provided to CSE under Non-disclosure Agreements (NDA) is accurate.

2.5 PROCESS

Before a CSE CSP ITS assessment can be completed, the following preliminary actions must be completed:

- Confirm or establish an NDA between CSE and the CSP being assessed. The documentation will be written and following discussions with the CSP will be conducted in accordance with the NDA.
- Confirm the GC client target security categorization and cloud security control profile.
- Obtain current and relevant reports from the CSP for the service being assessed.

The CSE CSP ITS assessment will be conducted in the following four phases:

Phase 1 – Confirmation of Attestation Documents

An initial review will be done to determine if the attestation reports received from the CSP address the required CSP security controls and enhancements in accordance with the selected security control profile. The review will identify the following items:

- Missing or unclear information
- Concerns that may need immediate discussions with the CSP

While these concerns are examined and the missing documentation is obtained, the remaining assessment work will continue wherever possible. Discussions with representatives from the CSP will continue throughout the assessment process.

Phase 2 – Detailed Evidence Review

The CSP-provided documentation will be examined to identify evidence of each of the selected ITS controls and enhancements. This examination will determine if the following conditions are met:

- The GC ITS requirements, as defined by *ITSG-33,* have been met.
- The CSP security services and procedures meet the GC-designated control and enhancement assignments.
- The documentation provides sufficient assurance that the CSP security services are implemented, operated, and maintained appropriately.

In addition, the CSE assessment team must review the CSP-provided documentation to determine if any of the following ITS recommendations or concerns apply:

- Is the CSP cloud fabric protected?
- Is the CSP corporate network separated from the cloud fabric to be used by the GC?
- Will the CSP management systems communicate with GC IT management networks and systems?
- Are GC systems and information separated and protected in a multi-tenant environment?
- Will GC users connect and authenticate to the IT services and information hosted by the CSP?
- Are there any policies, practices, services, or configurations that the GC clients must implement to enable the CSP security configurations?
- Are there any additional contractual terms that should be included in the procurement documentation?

Phase 3 – Initial Report and Supplementary Documentation

An initial report must be produced and shared with the CSP and the GC client. Based on the findings in this initial report, the CSP will be asked to clarify, provide additional evidence, or suggest measures to correct identified deficiencies. The GC client will be able to use the initial report to identify additional concerns, indicate where they are able to plan for implementation of security services identified as customer responsibilities, consider contract changes, and accept risks.

During this phase, the CSE assessment team will work with the CSP and GC client representatives to achieve a level of residual risk acceptable to all parties.

Phase 4 – Final Report

Once the processes in Phase 3 have reached a stage where all parties are prepared to move forward with the cloud security risk management process, a final report must be produced. The final report will include a summary of all CSE CSP ITS findings, and the recommendations and will be shared with both the CSP and GC client representatives.

Some public cloud services, including those that support GC enterprise IT, will need to be re-evaluated periodically.
CSE will provide recommendations to the GC client as to how often their public cloud services should be reassessed and respond to following GC client re-assessment requests.

3 REPORTING AND COMMUNICATIONS

We anticipate the following level of reporting and communications between the CSP, GC client, and CSE representatives:

3.1 REPORTS

Phase 1 – The CSE Assessment Team must send a short summary report to provide immediate indicators or notes about the CSP-provided documentation and potential ITS concerns.

Phase 2 – No reports are generated in this phase. The CSE assessment team will maintain communications with the CSP and GC client representatives to clarify requirements, questions, and concerns.

Phase 3 – The Initial Report must be sent to the CSP and GC client representatives. Subsequent meetings to review the findings with these representatives will be held to determine a way forward and address any concerns, recommendations, or questions raised in the Initial Report.

Phase 4 – Once approved by CSE management, the Final Report must be sent to the CSP and GC client representatives. Questions and concerns resulting from the Final Report may be addressed to the CSE assessment team lead. GC client organization will use the results of the Final Report as part of their cloud security risk management process.

3.2 COMMUNICATIONS

To monitor and protect the documentation that the CSE team needs to complete these assessments, a designated mailbox will be established for submission of documents to CSE. This mailbox will be controlled by the CSE Assessment Team Lead or a delegate. All CSP ITS assessment documentation will be managed and protected in accordance with CSE Information Management policies.

4 SUPPORTING CONTENT

4.1 LIST OF ABBREVIATIONS

Term	Definition
AICPA	American Institute of Certified Public Accountants
CCM	Cloud Controls Matrix
CSE	Communications Security Establishment
CSP	Cloud Service Provider
FedRAMP	Federal Risk and Authorization Management Program
GC	Government of Canada
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IT	Information Technology
ITPIN	Information Technology Policy Implementation Notice
ITS	Information Technology Security
MITS	Management of Information Technology Security
NDA	Non-Disclosure Agreement
PB/M/M	Protected B / Medium Integrity / Medium Availability
SOC	AICPA Service Organization Controls
SSP	System Security Plan
TBS	Treasury Board of Canada Secretariat

4.2 GLOSSARY

Term	Definition
Attestation	Any ITS-related certification or assessment to which CSPs may subject their services.
Availability	The state of being accessible and usable in a timely and reliable manner. [1]
Cloud	Cloud computing is a model for enabling anywhere, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. [5]
Cloud fabric	The servers, hi-speed connections, and switches that make up a cloud computing platform or framework.
Confidentiality	The state of being disclosed only to authorized principals. [1]
Control Profile	A set of security controls and enhancements that establishes the minimum security requirements for an information technology function and supporting information systems. [1]
Deployment Model	The purpose for which the cloud infrastructure is provisioned as determined by the intended user communities. See Special Publication 800-145, *The NIST Definition of Cloud Computing* for additional information [5]
Integrity	The state of being accurate, complete, authentic, and intact. [1]
Multi-tenant Environment	An information system environment where physical and virtual resources are dynamically assigned and reassigned to serve multiple customers.
Risk Management	A systematic approach to setting the best course of action under uncertainty by identifying, assessing, understanding, making decisions on and communicating risk issues.
Security Control	A management, operational, or technical high-level security requirement prescribed for an information system to protect the confidentiality, integrity, and availability of its IT assets. [1]
Security category	A security category characterizes a business activity by the severity of expected injuries (injury level) from compromise with respect to the security objectives of confidentiality, integrity, and availability. [1]
Service Model	The capability that is provided to the cloud consumer. See Special Publication 800-145, *The NIST Definition of Cloud Computing* for additional information [5]

4.3 REFERENCES

Number	Reference
1	Communications Security Establishment. *ITSG-33*. *IT Security Risk Management: A Lifecycle Approach,* December 2014.
2	Treasury Board of Canada Secretariat. *GC Security Control Profile for GC Cloud-based IT Services Protected B, Medium, Medium, Version 1.1*. 28 March 2018.
3	Treasury Board of Canada Secretariat, *Policy on Information Management,* 29 March 2018..
4	Treasury Board of Canada Secretariat. *Policy on Management of Information Technolog,. 29* March 29 2018.
5	National Institute of Standards and Technology. *Special Publication 800-145, The NIST Definition of Cloud Computing*. September 2011.
6	Treasury Board of Canada Secretariat. *GC Cloud Security Risk Management Approach and Procedures v1.3*, 6 June 2018