Cloud Security Evaluation Approaches

By Vidushi Gupta

Introduction

Cloud computing allows information to be delivered in a flexible and an agile manner. With the process of operating under cloud computing services provided by a cloud service provider (CSP), governments renounce control over many aspects of security and privacy. Therefore, appropriate evaluation measures must be taken to establish trust between CSPs and governments. The following test explores different methods employed by agencies to this end. Specifically, assessment methods used by Government of Canada (GC) before partnering with commercial CSPs to host government applications over, are explored. Compliance with cloud security standards are instrumental in establishing trust and thus FedRAMP, a standard used by government of United States to evaluate CSPs is discussed. Differences and similarities between evaluation methods used by FedRAMP to certify CSPs and those used by GC to determine host CSPs are described. Another standard called Common Criteria(CC) is used. Common criteria while explicitly, not for standardizing cloud services but IT products in general offers guidelines about security requirements that are used by FedRAMP. Hence, notable assessment methods used by CC are discussed.

Abbreviations

GC- Government of Canada

CSP-Cloud Service Provider

CCCS-Canadian Centre for Cyber Security

ITS-Information Technology Security

SAF-Security Assessment Framework

SAR- Security Assessment Report

FedRAMP-Federal Risk and Authorization Management Program

TBS–Treasury Board of Canada Secretariat

NIST-National Institute of Standards and Technology

SSP-System Security Plan

CC-Common criteria

NAIP–National Information Assurance Partnership

ITSG – IT Security Risk Management

ISO – International Standards Organisation

FedRAMP

FedRAMP is a government wide program in US that provides a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services." (FedRAMP, n.d.). While GC favors compliance with ITSG-33 (Canadian Centre for Cyber Security (CCCS), 2018)and TBS' cloud security profile (Treasury Board of Canada Secretariat, 2016), there is no certificate specifically required by CSPs to be certified to provide cloud services to GC. Compliance with international standards of FedRAMP, ISO are accepted pending further assessment. However, US government demands FedRAMP compliance from CSPs that wish to sell cloud service to it (Executive Office of the President, Office of Management and Budget, 2011). Similar to GC requiring categorization of business activities into separate security profiles (Treasury Board of Canada Secretariat, 2016), FedRAMP defines a set of controls for low and moderate security impact level systems. (National Institute of Standard and Technology, 2004) provides detailed information about each category of security profile. Each category has security control requirements based on NIST baseline controls (National Institute of Standards and Technology, 2013). Some other standards that affect security controls and assessment process are mentioned in section 1.2 "Applicable Standards and Guidance" of FedRAMP Security Assessment Framework document (FedRAMP, 2017). FedRAMP has adopted these standard's requirements package and authorization packages that all assessment agencies and CSPs can use. Subsequent sections mention a few categories of requirements.

As per OMB memorandum (Executive Office of the President, Office of Management and Budget, 2011) CSPs who wish to provide cloud services to the government must be certified with FedRAMP. Consequently, CSPs are required to implement FedRAMP baseline security controls. CSPs support their compliance with FedRAMP by following FedRAMP's Security Assessment Framework (SAF) (FedRAMP, 2017). SAF aligns with the NIST Risk Management Framework (RMF) (NIST, 2018). FedRAMP simplifies the RMF by dividing risk management for cloud computing into four main processes document, assess, authorize and monitor. While the stages of assessment are similar to GC's assessment methods, notable differences are discussed.

Process of Assessment by FedRAMP

Phase 1: Document

After identifying security profile (i.e. High, Moderate, Low, Low-Impact software-as-a-service (SaaS)), CSPs implement security controls for their category. Full details of required security controls for all security profiles are provided in form of documents and templates on FedRAMP's website (FedRAMP, 2020). CSPs should complete a CSP information form (FedRAMP, n.d.) and submit a FedRAMP System Security Plan (SSP) according to low, moderate or high baseline templates (FedRAMP, 2018). Such a document is not found or needed for assessment by CCCS, as the former relies on a CSP to be pre-certified with FedRAMP.

FedRAMP acknowledges that CSPs might already have implemented security controls required by FedRAMP. However, evidence of their implementation must be provided. Additionally, CSPs may need to reconfigure implementations to suit requirements by FedRAMP. If intentions align, FedRAMP is flexible with implementation of security controls.

Similar to CCCS, FedRAMP acknowledges that some SaaS applications may obtain their infrastructure from Infrastructure as a service application and thus inherit the latter's security controls. In documentation submitted by CSP to FedRAMP during pre-authorisation phase, a CSP must only provide SSP for its own service and not for foundational infrastructure services.

Process 2: Assess

Pre-authorised third-party agencies assess security controls of a CSP independently with help of a Security Assessment Plan (SAP). Template of SAP is found on FedRAMP's website titled "Initial Authorization Phase- Assess: Security Assessment Plan (SAP)" (FedRAMP, 2017). Such a formal assessment document is not found on CCCS's website. Although since CCCS relies on FedRAMP procedures heavily, there is enough evidence to believe that a similar template is followed by CCCS security assessors during their assessment process. Some features of SAP template provided by FedRAMP are:

- Requires that data centre site name and address and description of components be documented. It is not clearly specified if these components are physical in nature. If physical components in a data centre are in fact tested, then this differs from assessment done by CCCS as CCCS does not test physical components.
- Requires that IP addresses, web application and data bases slated for testing be recorded.
- Requires that different authorization roles be tested to check if permissions assigned to each role are tested properly
- This template directs to test procedures to evaluate security control for high, moderate and low security profiles. These test procedures may be done through manual and automated tools. An example of manual test procedure is "Forceful Browsing" describes as "We will login as a customer and try to see if we can gain access to the Network Administrator and Database Administrator privileges and authorizations by navigating to different views and manually forcing the browser to various URLs." (FedRAMP, 2017). Test procedures are documented in an excel sheet publicly available (FedRAMP, 2017). Along with test procedures, this also contains test objectives and test cases.
- Ways to collect information from CSP being assessed are mentioned including but not limited to completed FedRAMP templates and supporting documents required to be submitted after travelling to CSP sites.
- Assessment methods are mentioned such as examining, interviewing and technical tests performed to test security of cloud architecture.
- Instructs on recording tools used for testing be recorded, including their purpose and vendor organisation.
- If manual testing is performed, it is required to document details and duration of test. There are procedures in place to record testing schedule and timeline.
- Finally, it must be decided how results of assessment will be communicated between assessing third party and CSP.

Phase 3: Authorise

A Security Assessment Report (SAR) must be produced after assessment procedures have been completed. A template for SAR is also available on FedRAMP website under "Initial Authorization Phase- Authorize: Security Assessment Report (SAR)" (FedRAMP, 2017). The

SAR describes vulnerabilities, threats, and risks discovered during the testing process. Additionally, the SAR contains guidance for CSPs in mitigating the security weaknesses found. A list of potential threats is documented in SAR template. Some examples are alteration of data, files and records, data disclosure attack etc. Their degree of impact on confidentiality, integrity and availability are mentioned.

After receiving SAR, a CSP makes a "Plan of Action & Milestones" document to address vulnerabilities and risk observed in risk analysis reported in SAR. Following, CSP submits a security package that is reviewed again for final authorisation.

A CSP is free to elect a third-party assessor that has not been pre-authorised by FedRAMP. In that case, the agency's credentials describing its independence and technical qualifications must be submitted to FedRAMP.

Government of Canada

Government of Canada (GC) seeks compliance with Federal Risk and Authorization Management Program (FedRAMP) from Cloud Service Providers (CSP) among other standards. GC has established an evaluation and risk management strategy for cloud environments that defines procedures to assess security of a CSP based on established standards and against its own set of security controls (Government of Canada, 2019). Notable aspects of "Government of Canada Cloud Security Risk Management Approach and Procedures" are described in subsequent sections.

Process of Assessment by GC

According to GC's Cloud Security Risk Management Approach (Canadian Centre for Cyber Security, 2019)**,** GC holds itself responsible for security of information services on the cloud, including those provided by external CSPs. A four-stage process is implemented to this end. Each stage involves collaboration of CSP and GC. This process is diagrammatically represented in figure 1 and processes are described in subsequent texts.

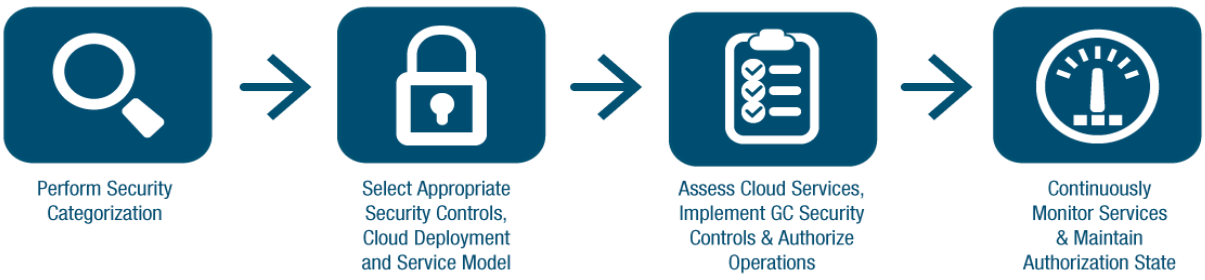

Figure 1: GC Cloud Security Risk Management Process

Security Categorization: To initiate security categorization, GC department identifies information related to business processes or services provided by GC service. Afterward, these activities are categorised on degrees of loss of confidentiality, integrity and availability to national and non-national threats in the event of a security compromise. Figure 2 below shows this categorisation process in diagram form.

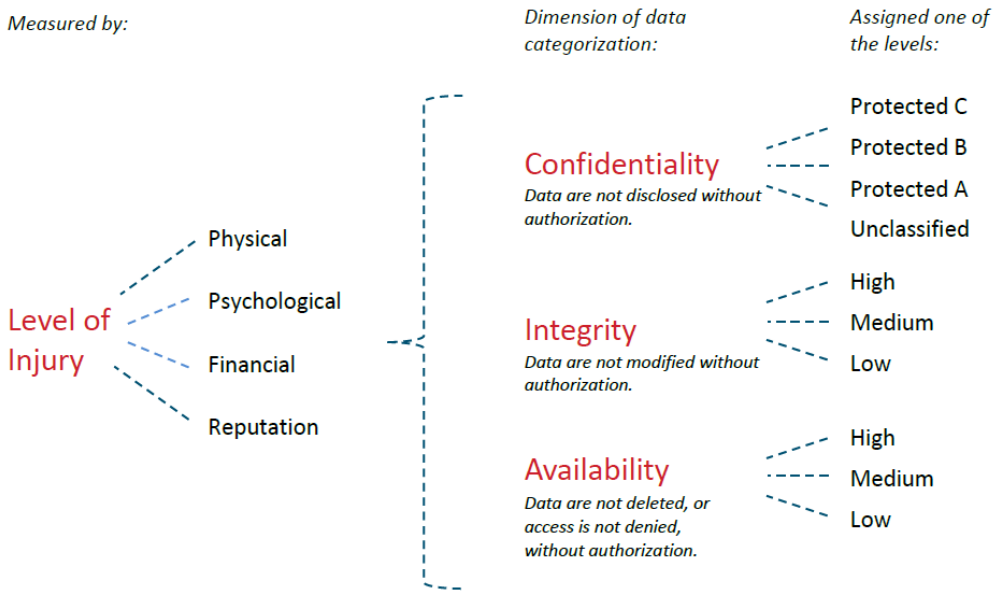

Figure 2: Security Categorization of Information Assets of a GC Department

Selecting Appropriate Security Controls: Following on type of security category a GC's information assets falls into, the GC selects an appropriate security control profile. "A security control profile specifies for implementation a set of security controls to protect information systems supporting specific business activities when operating in specific technical and threat contexts by following specific security approaches." (Government of Canada, 2019). This process is applicable for range of IT products and services including cloud services. Security requirements for two types of security profiles are specified in "IT Security Risk Management: A Lifecycle Approach (ITSG-33)" published by Canadian Centre for Cyber Security (Canadian Centre for Cyber Security (CCCS), 2018). These security controls are applicable to all IT services including cloud. Specific cloud services security controls are documented in Treasury Board of Canada's Security Control Profile for Cloud-based GC Services in form of a template that can be asked for by emailing GC (CCCS, 2018). This document is not posted online due to its length (Government of Canada, 2016). Comparatively, FedRAMP provides similar baseline security controls for cloud services in form of a template which can be downloaded directly from FedRAMP's website (FedRAMP, 2018). Two types of security profiles are specified in "IT Security Risk Management: A Lifecycle Approach (ITSG-33) are:

- PROTECTED B / Medium Integrity / Medium Availability (PB/M/M) (Government of Canada, 2018): Protected B level of confidentiality indicates that access to PROTECTED B information is reasonably expected to cause a medium level of injury to non-national interests. Examples of business contexts applicable to this profile are provided. Categories of deliberate threat, Accidental Threats and Natural Hazard are detailed along with suggested security controls and Control Enhancements.
- SECRET / Medium Integrity / Medium Availability (CCCS, 2018): SECRET level of confidentiality indicates that access to SECRET information is reasonably expected to

cause a high level of injury to national interests. Business categories, threat categories and suggested security controls are provided in detail.

FedRAMP also divided cloud services into low, medium, high impact. Security requirements mentioned in security category profiles support compliance to GC legislation and Treasury Board of Canada Secretariat (TBS) policies, directives, and standards related to the protection of information systems (CCCS, 2018). If a department cannot identify requirements suitable to its security profile, security practitioners must create requirements for department from catalogue of security controls mentioned in Annex 3A of ITSG-33 (CCCS, 2018). Security controls chosen personally for a security profile must be compliant with GC legislation and TBS policies, directives, and standards. Similarly, FedRAMP also categorises on low and moderate impact level profiles. Details of these profiles are be obtained from FIPS PUB 299 publication (National Institute of Standards and Technology , 2004). Upon further research, security profiles derived by CCCS are very similar to those derived by FedRAMP.

Assessment: To uphold accountability, independent third-party security assessors confirm compliance with relevant standards. This process is elaborated in Cloud Service Provider Information Technology Security Assessment Process document (ITSM.50.100) (CCCS, 2018) . A similar document is provided by FedRAMP (FedRAMP, 2017). Differences between assessment approaches is discussed in later sections. Established by Canadian Centre For Cyber Security (CCCS), the purpose of this document is to help GC's departments and services in evaluating cloud services obtained from CSPs for use by GCs. Currently, both by FedRAMP and CCCS, security profiles with low and medium impact levels are covered. Services whose security breach can have high impact are not delegated to cloud services and use local resources (Government of Canada, 2016).

GC recognises specific international information technology security certificates if a CSP has been pre-authorised under them. To ensure authenticity of these certificates, independent third parties verify compliance. Comparatively, FedRAMP provides a Joint Authorisation Board which acts as alternative path to authorisation.

Main parameters that security is assessed against are TBS cloud security profile (Government of Canada, 2016) and industry standards that are specifically listed to be:

- System Security Plans (SSP) produced for FedRAMP
- AICPA SOC 2 Type II reports
- ISO/IEC 27001 reports
- ISO/IEC 27017 reports

Other standards are not currently recognised to form part of common review parameters for CCCS CSP security assessments (CCCS, 2018). In case, the CCCS assessment team is not satisfied with security controls that are certified, other formal certifications may be requested and, in their absence, risk mitigation measures are negotiated. The assessment process comprises of following four phases:

Phase 1: Confirmation of Attestation Documents

Done by GC department personnel looking for contract with CSP. CSP representatives are present to provide answers

Based on common criteria established between TBC security control profile as selected (PB/M/M or below) and listed international standards.

Goal: Identify if information is missing or unclear and other concerns to discuss with CSP.

Phase 2: Detailed evidence review

Done by: CCCS assessment team

Based on: ITSG-33 and GC cloud security profile requirements for respective security profile. ITSG-33 is available online (Canadian Centre for Cyber Security (CCCS), 2018). However, the template for GC cloud control requirements, due to size is not available online and needs to be requested to be sent through email (CCCS, 2018) . This document mentions requirements, a brief description and records its compliance with ITSG-33, NIST and FedRAMP standards among others. As mentioned before, ITSG-33 is risk management profile is applicable to all IT services. Requirements for cloud services specifically are mentioned in GC cloud control requirements template. The CCCS assessment team delves into finer security details in the phase. Specific questions are asked such as security of separation between CSP management and GC services and process of authentication for GC users.

Goal: In addition to identifying missing or unclear criteria from, phase 2 attempts to identify to probe further about any additional concerns.

Phase 3: Initial report and supplementary documentation

Done by: CCCS assessment team

Based on a preliminary assessment report produced after phase 2. This report shared with both CSP and GC client.

Goal: This report is used to ask CSP for additional clarifications, provide evidence, suggest measure to amend identified deficiencies. GC client will use report to accept risks, plan and indicate how they will implement security measures that are a customer's responsibility, and ask for changes in contract. The CCCS team will work with both parties to negotiate risk that is acceptable to both parties.

Phase 4: Final report

Done by: CCCS assessment team

Based on findings from initial report evaluation in phase 3.

Goal: To summarise findings, risks, responsibilities. Based on recommendation from CCCS, it also established if there is need to re-evaluate security parameters periodically.

Limitations: (CCCS, 2018)

- Profiles identified with high impact levels with confidentiality, availability or integrity are not assessed because providing these services using cloud is not pursued.
- Verifying physical security requirements of data centres in Canada is outside the scope of this approach.
- personnel employed by CSP to support services in Canada are not verified to have appropriate security personnel requirements
- Privacy requirements are restricted to protection of confidentiality, integrity and availability of GC information. FedRAMP also follows similar ideas of privacy based on confidentiality, integrity and availability (FedRAMP, 2017)
- There is little automation with assessment process. Fair amount of resources of CCCS are engaged during assessment process. Comparatively, FedRAMP delegates pre-authorization tasks to CSPs by providing documents and templates (FedRAMP, n.d.).

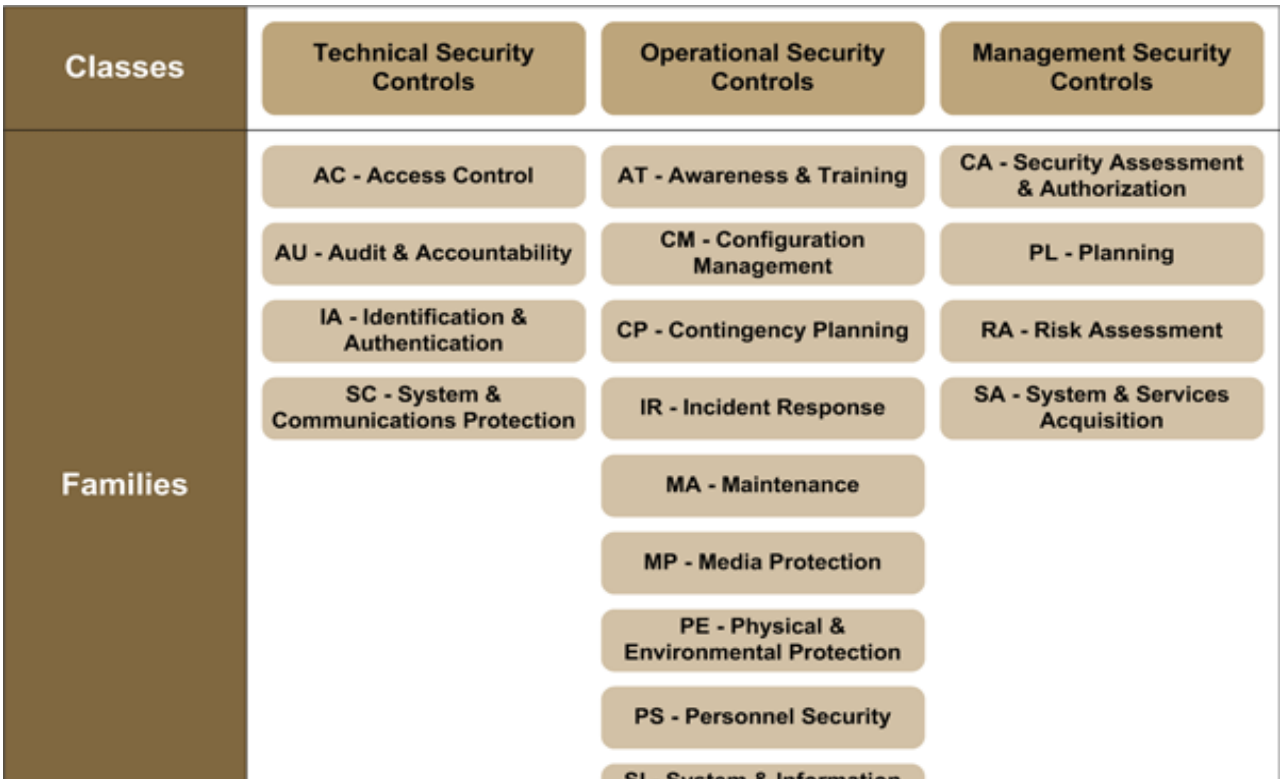

Figure 3: Security requirements of FedRAMP and CCCS divided intro families and classes (CCCS, 2018)

Security Control Requirements of FedRAMP and CCCS

FedRAMP's security requirements for cloud security are based on NIST 800 series security controls. An excel sheet template is available on FedRAMP's website that divides requirements into low, medium and high baseline controls (FedRAMP, 2018). There are divided into families such as access control, audit and accountability among others. Security control catalogue mentioned under ISTG-33 (CCCS, 2018)are like those of FedRAMP and consequently based on NIST 800 series. Each security control is assigned a unique security control number. All security controls starting at 100 (e.g. SC-100, SC-101) are Canadian specific security controls. Figure 3 shows security control categories divided into families and classes (CCCS, 2018).

Comparison between assessments of CSPs by FedRAMP and GC/CCCS

- In order to provide services to federal government, CSPs must be certified with FedRAMP as a necessary requirement. However, to provide services to GC, CSPs may be certified with FedRAMP, ISO/IEC 27001, ISO/IEC 27017, AICPA SOC 2 Type II reports.
- Unlike CCCS, which highlight limitations of their assessment process (CCCS, 2018), FedRAMP does not mention limitations in their assessment process. Therefore, it in unclear if they check physical security of components in a data center or if CSP employees are verified to perform roles that give them access to confidential government information.
- CSPs seeking to get authorized with FedRAMP work closely with partnership third-party agencies. FedRAMP's officials are involved mostly during authorization and have limited role during pre-authorization and post-authorization phases. Comparatively, CCCS personnel are part of assessment process through all phases.
- For requirements and test procedures, FedRAMP draws heavily from established standards by NIST and Common Criteria. Templates are provided with sample test procedures, their assessment objectives (FedRAMP, n.d.). (FedRAMP, 2017) provides a sample test case procedure template file in form of an excel sheet. GC's relies on assessment done by FedRAMP and therefore, do not provide templates or documents for test procedures. Their requirements, however, are based on NIST and Common Criteria also.
- Procedures to record timeline of each phase of assessment are not mentioned in CCCS assessment. Comparatively, FedRAMP asks for timeline to be recorded in Security Assessment Report template (FedRAMP, 2017)

Common Criteria (CC) (Common Criteria, n.d.)

"The Common Criteria is an international program in which accredited laboratories test IT products against standard cyber security specifications called Protection Profiles (PPs). " (Canadian Centre for Cyber Security, 2018). Presently, 31 countries are members of CCRA (common criteria recognition arrangement) including Canada and USA. These countries agree to common set of requirements to evaluate IT products. The objective is to avoid redundant evaluations in different countries and to increase quality of evaluations. While CC addresses all types of IT technologies, FedRAMP security requirements for cloud security is influenced by CC. Security requirements in low baseline security controls template (FedRAMP, 2018), products that CC certified are recommend. For example, within System and Services Acquisition Criteria, SA-05, Acquisition Process, it is recommended to use products certified by common criteria (ISO/IEC 15408). CC is kept intentionally flexible to allow use in different IT services.

CC allows compatibility between results of independent security evaluations. (Criteria, Common, 2017) specifies security requirements, classified into classes and families. This categorisation is same as that in FedRAMP and CCCS. This is additional evidence that FedRAMP and CCCS derive requirements from CC due to universal applicability of CC. Some examples of classes are mentioned below. Details of these requirements can be found on (Criteria, Common, 2017).

- Relating to Security audit: security audit automatic response, security audit data generation requirements, security audit analysis
- Cryptographic support: cryptographic key management. Cryptographic operation
- User data protection: Access control policy, Access control functions

- Identification and authentication: requirements in case of authentication failures, user attribute definition, user-subject binding

(Common Criteria, 2017)defines evaluation criteria for different protection profiles and defines a scale to grade security levels of an IT service. Protection Profiles are discussed briefly under "Protection Profile Evaluation" section of (Common Criteria, 2017). While requirements are listed in (Criteria, Common, 2017), security assurance document divides evaluation into different facets of security components and describes information expected to be provided to the evaluator. Also, it describes methods to communicate and document successful compliance to requirements. CC evaluation components are meant to act as guidelines to assessing bodies in member countries. CC is intentionally flexible. Therefore, a range of evaluation methods can be used to test security properties of many IT products including those employed for cloud services.

Some other facets as part of IT product assessment according to CC are:

Protection Profile Evaluation: IT products certified with common criteria, are concerned with a specific technology, for example operating systems or key management systems among others. Security requirements of these technologies are specified in Protection Profiles (Common Criteria, n.d.). Some examples of protection profiles are secure messages protection profile, protection profile for enterprise security management access control (Booz Allen Hamilton, 2013). These profiles have been certified according to common criteria of assurance level of evaluation. While these products are not classified under cloud computing, these technologies (e.g. cryptography) can be part of cloud computing architecture.

Protection Profile Configuration Evaluation provides procedures to determine if protection or security profile has been identified correctly.

Security target evaluation: recording conformance claims, security problem definition and security objectives is required.

Development: consists of security architecture, implementation representation

Life cycle support: Delivery, development security, flaw remediation

Testing: gives information on how test should be conducted, and results recorded.

Vulnerability assessment: Vulnerability analysis

As part of security assurance in Security Assurance Components document (Common Criteria, 2017), assurance levels and criteria for permitting attestation at each level are mentioned.

- Level 1: functionally tested
- Level 2: Structurally tested
- Level 3: Methodically tested and checked
- Level 4: Methodically designed tested reviewed
- Level 5: Semi formally designed and tested
- Level 6: Semi formally verified design and tested
- Level 7: Formally verified design and tested

IT products are assessed and certified under common criteria. (Common Criteria, n.d.) gives a list of certified products categorised according to functionality and use.

For example, under “network and network related devices and systems” a SDN technology called Big Switch Networks’ Big Cloud Fabric 4.7.0 Security Target was evaluated using common criteria assessment methods by a third authorised party in Spain (CERT10, 2018). Specifically, the product was evaluated to fulfill requirements of Level 2 assessment. In this evaluation, key security features such as role management, tenant isolation, multiple authentication schemes were evaluated. Requirements are divided into classes derived from common criteria requirement v3.1R5 (Criteria, Common, 2017). For instance, under cryptographic requirements, each cryptographic operation with cryptographic algorithm, key size is mentioned in detail and in tabular form (Corsec, 2018). Evaluation steps are documented in detail in certification report available specifically for this product (CERT10, 2018) and all other products on common criteria website. Security practitioners looking to employ IT products can peruse security target and evaluation documents to obtain details of protection profiles and evaluation results.

Products that pursue certification with common criteria are sent to licensed labs (Common Criteria) for evaluation. They are authorised by certificate authorising schemes (Common Criteria, n.d.). As an example, in United States, the authorizing scheme is National Information Assurance Partnership (NIAP) (National Information Assurance Partnership, n.d.). To obtain a CC certificate from NIAP, a product vendor chooses an approved protection profile and designs a draft security target. A licensed lab evaluates these security targets and produces an evaluation report which is finally sent to NAIP to complete certification. NAIP allows labs to choose their process of evaluation and reviews evaluation reports. Unlike FedRAMP, guidance templates and documents to provide guidance to CSP vendors are not available. The Leidos Accredited Testing & Evaluation laboratory (Overview of CC evaluation, n.d.) provides overview of protection profile evaluation and consulting, and assurance evaluation services. However, no clear evaluation criteria in the form of test procedures, criteria are mentioned.

Conclusion

GC does not explicitly recognise common criteria certification to evaluate CSPs. However, like FedRAMP, products certified by CC are preferred over non-certified counterparts. FedRAMP is comprehensive and formal. There are processes such as documents and templates available that automate and delegate the process of assessment between CSPs, third party assessors and Fedramp officials. GC’s assessment of CSPs relies heavily on compliance with FedRAMP and ISO/IEC 27001, 27017. Therefore, there is reason to view it as an additional layer of evaluation. Automated processes are few and a more hands-on approach is observed by CCCS primarily performing the assessment. FedRAMP aims to save resources during cloud security assessments by being repeatable.CC, however, provides guidelines and relies on licensed labs to perform their own assessment. FedRAMP and CC requirements are derived from NIST standards. Future work involves exploration of NIST and its influence on cloud security evaluation methods in difference countries of the world.

References

CERT10. (2018, December 11). *Certification Report for Big Switch Networks Big Cloud Fabric 4.7.0.* Retrieved from https://www.commoncriteriaportal.org/files/epfiles/2017-23-INF-2630.pdf

Booz Allen Hamilton. (2013). *Protection Profile for Enterprise Security Management Access Control*. Retrieved from Common Criteria Official Website: https://www.commoncriteriaportal.org/files/ppfiles/pp_esm_ac_v2.1.pdf

Canadian Centre for Cyber Security (CCCS). (2018, November 5). *Table of Contents: IT Security Risk Management: A Lifecycle Approach (ITSG-33)*. Retrieved from Canadian Centre for Cyber Security: https://cyber.gc.ca/en/guidance/it-security-risk-management-lifecycle-approach-itsg-33

Canadian Centre for Cyber Security. (2018, September 30). *Introduction of Common Criteria*. Retrieved from https://cyber.gc.ca/en/common-criteria

Canadian Centre for Cyber Security. (2019, March). *Cloud Security Risk Management*. Retrieved from https://cyber.gc.ca/en/guidance/cloud-security-risk-management-itsm50062

CCCS. (2018, September 26). *Annex 3A - Security Control Catalogue (ITSG-33)*. Retrieved from https://cyber.gc.ca/en/guidance/annex-3a-security-control-catalogue-itsg-33

CCCS. (2018, September 25). *Annex 4A - Profile 3 - (SECRET / Medium Integrity / Medium Availability) (ITSG-33)*. Retrieved from https://cyber.gc.ca/en/guidance/annex-4a-profile-3-secret-medium-integrity-medium-availability-itsg-33

CCCS. (2018). *Cloud Security Control Recommendations (Version 1.1).*

CCCS. (2018). *Cloud Service Provider Information Technology Security Assessment Process*. Retrieved from https://www.cyber.gc.ca/sites/default/files/publications/itsm.50.100-en.pdf

Common Criteria. (2017, April). *Security assurance components: Common Criteria*. Retrieved from https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5_marked_changes.pdf

Common Criteria. (n.d.). *Certificate Authorizing Schemes*. Retrieved from https://www.commoncriteriaportal.org/ccra/schemes/?CFID=49174594&CFTOKEN=653a40bbadb041b0-87EC4830-155D-00D0-0A2214C4BB7C84CE

Common Criteria. (n.d.). *Certified Products: Common Criteria*. Retrieved from https://www.commoncriteriaportal.org/products/

Common Criteria. (n.d.). *Common Criteria Home Page*. Retrieved from https://www.commoncriteriaportal.org/

Common Criteria. (n.d.). *Licensed Laboratories.* Retrieved from https://www.commoncriteriaportal.org/labs/

Common Criteria. (n.d.). *Protection Profiles: Common Critera*. Retrieved from https://www.commoncriteriaportal.org/pps/

Corsec. (2018, October). *Security Target for Big Switch Networks*. Retrieved from https://www.commoncriteriaportal.org/files/epfiles/2017-23-ST.pdf

Criteria, Common. (2017, April). *Security functional requirements:common criteria* . Retrieved from https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5_marked_changes.pdf

Executive Office of the President, Office of Management and Budget. (2011, December 8). *MEMORANDUM FOR CHIEF INFORMATION OFFICERS.* Retrieved from FedRAMP official website: https://www.fedramp.gov/assets/resources/documents/FedRAMP_Policy_Memo.pdf

FedRAMP. (2017, October 3). *FedRAMP High Security Test Case Procedures Template.* Retrieved from https://www.fedramp.gov/assets/resources/templates/SAP-AA-FedRAMP-High-Security-Test-Case-Procedures-Template.xlsx

FedRAMP. (2017, June 6). *FedRAMP Security Assessment Plan (SAP) Template.* Retrieved from https://www.fedramp.gov/assets/resources/templates/FedRAMP-SAP-Template.docx

FedRAMP. (2017, June 6). *FedRAMP Security Assessment Report (SAR) Template.* Retrieved from https://www.fedramp.gov/assets/resources/templates/FedRAMP-SAR-Template.docx

FedRAMP. (2017, November 15). *Security Assesment Framework document: FedRAMP.* Retrieved from FedRAMP official website: https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Assessment_Framework.pdf

FedRAMP. (2017, November 16). *Understanding Baselines and Impact Levels in FedRAMP*. Retrieved from https://www.fedramp.gov/understanding-baselines-and-impact-levels/

FedRAMP. (2018, October). *Documents provided by FedRAMP*. Retrieved from https://www.fedramp.gov/documents/

FedRAMP. (2018, September 28). *FedRAMP Security Controls Baseline.* Retrieved from FedRAMP official website: https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Controls_Baseline.xlsx

FedRAMP. (2018, August 28). *FedRAMP System Security Plan (SSP) Low Baseline Template.* Retrieved from https://www.fedramp.gov/assets/resources/templates/FedRAMP-SSP-Low-Baseline-Template.docx

FedRAMP. (2020). *Templates provided by FedRAMP*. Retrieved from https://www.fedramp.gov/templates/

FedRAMP. (n.d.). *FedRAMP CSP Information Form*. Retrieved from https://docs.google.com/forms/d/e/1FAIpQLScU4_x5UK53d0PUUDsOdqWyzUvAN1-yFJ1NxffT7PkGkCiuPg/viewform

FedRAMP. (n.d.). *Guidance for Cloud Service Providers*. Retrieved from https://www.fedramp.gov/cloud-service-providers/

FedRAMP. (n.d.). *Home page FedRAMP*. Retrieved from FedRAMP official website: https://www.fedramp.gov/

FedRAMP. (n.d.). *Templates*. Retrieved from FedRAMP official website: https://www.fedramp.gov/templates/

Government of Canada. (2016). *Government of Canada Security Control Profile for Cloud-based GC Services*. Retrieved from https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-services/government-canada-security-control-profile-cloud-based-it-services.html

Government of Canada. (2018, September 25). *Annex 4A - Profile 1 - (PROTECTED B / Medium Integrity / Medium Availability) (ITSG-33)*. Retrieved from https://cyber.gc.ca/en/guidance/annex-4a-profile-1-protected-b-medium-integrity-medium-availability-itsg-33

Government of Canada. (2019, June 17). *Cloud Security Risk Management Approach and Procedures*. Retrieved from Government of Canada website: https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-services/cloud-security-risk-management-approach-procedures.html#toc3

National Information Assurance Partnership. (n.d.). *Evaluation Process*. Retrieved from https://www.niap-ccevs.org/Ref/Evals.cfm

National Institute of Standard and Technology. (2004, February). *Cloud Service Providers: FedRAMP.* Retrieved from FedRAMP government website: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

National Institute of Standards and Technology . (2004). *FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems*. Retrieved from https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

National Institute of Standards and Technology. (2013, April). *Security and Privacy Controls for Federal Information Systems and Organisations.* Retrieved from NIST official website: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

NIST. (2018, December). *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. Retrieved from NIST website\: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

Overview of CC evaluation. (n.d.). Retrieved from https://www.leidos.com/sites/g/files/zoouby166/files/2020-02/FS-Accredited-Testing-Evaluation.pdf

Treasury Board of Canada Secretariat. (2016). *GC Right Cloud Selection Guidance.* Ottawa: Government of Canada.