Final Project Report

Comparative Analysis of Existing Approaches for Evaluating Cloud Security

By Vidushi Gupta

A. Introduction

Cloud computing allows information to be delivered in a flexible and agile manner. By using cloud services operated by a cloud service provider (CSP), organizations renounce control over many aspects of security and privacy. Therefore, it is important that organizations trust a CSP to keep data secure. To promote trust, CSPs are evaluated against a standard set of requirements. International Organization for Standardization(ISO) (International Organization for Standardization, 1947), Control Objectives for Information and Related Technology (COBIT) (ISACA, 2019), Federal Risk and Authorization Management Program (FedRAMP) are some standards that contain security requirements that a CSP is evaluated against. In this report, we will be focusing on three standards called FedRAMP, Common Criteria (CC) (Common Criteria, n.d.), Information Technology Security Guidance (Canadian Centre for Cyber Security (CCCS), 2018). Based on methodology described in Report #3 on Comparative Analysis Methodology (Gupta, 2020) and summarized in “Methodology” section, these standards will be evaluated. Starting with introduction in section A, section B describes purpose of comparison between standards of cloud security, section C describes methodology for performing evaluation, section D performs evaluation, section E compares results of evaluation between different standards, section F derives conclusions from evaluation. Finally, section G concludes the report. To avoid repeating information, references are provided to relevant sections and previous reports.

B. Purpose

This report seeks to evaluate cloud standards based on criteria introduced in report #3 (Gupta, Comparative Analysis Methodology, 2020). This evaluation is useful for CSP personnel and security practitioners researching between different standards for cloud computing security with the goal of certification or for information purposes. The criteria introduced also allow comparison between different security standards. A CSP or an IT product developer pursuing certification may use this evaluation criteria to decide which standards to comply in addition to gaining information about important aspects that define a standard. Results of evaluation provide detailed knowledge about attributes such as security requirements, assessment processes, transparency, flexibility and repeatability. These qualities distinguish one standard from another. Furthermore, evaluation is useful for clients looking to contract CSPs to conduct business activities and provide services. Depending on functionality of client product, flexibility with requirements, procedures to address new vulnerabilities, presence of certain type of requirements (e.g. cryptography) may be demanded. In that case, a client may use evaluation results to choose standard that best suits their product. They may then hire a CSP compliant with preferred standard.

Reasons for choosing to detail CC, FedRAMP and ITSG-33 is threefold. Firstly, resources explaining these standards such as documents about requirements, assessments, templates are publicly available.

Secondly, these standards certify not only CSPs but all IT products. This broadens our perspective into security standards for IT products and their relation to cloud products. For example, audit requirements are required to be fulfilled not just for CSPs but IT products in general. This also raises the question if a separate standard is required for cloud products or do standards with requirements for IT products suffice. Thirdly, as will be mentioned later in the report, FedRAMP and ITSG-33 are mandatory requirements for products looking to supply services to the government. We are of the opinion that governments of countries are a strong customer base with many security challenges and hence are interested in standards pertaining to them.

Our evaluation criteria are limited in that finer points of comparison are not included. This led to an evaluation criteria that can be applied to a wide variety of security standards while providing all relevant information to fulfill purpose of evaluation. Comparing smaller details between standards was outside the scope of this study. For example, comparison between specifics of assessment tests to evaluate differences has not been done. Also, such specifics are not always described in a standard. Assessment teams are given flexibility to decide based on type of product. Evaluation criteria focuses on revealing differences in aspects/procedures/processes and does not discuss similarities in detail.

C. Methodology adopted

Report #3 (Gupta, 2020) introduced metrics that are used as criteria to evaluate a standard. The evaluation criteria formed questions which are answered using yes/no. Evaluation criteria are divided into those related to security profiles, security requirements, privacy, flexibility criteria, transparency, assessment process and continuous monitoring or reassessment. This is because these attributes of a standard distinguish it from other standards in terms of applicability, easy implementation, transparency, repeatability.

To evaluate a standard, questions are provided that can be answered in yes/no capacity. Resources are provided by a standard to offer answers. If appropriate resources are not available to answer a question, "No information available" is written. Lack of resources is also investigated as criteria for judging a standard.

D. Detailed Evaluation

Evaluation criteria is applied on CC, FedRAMP and ITSG-33 in detail. To avoid repeating information provided in previous reports, relevant references are provided

Common criteria

Security Profile Criteria

1. *Are documents/templates provided by standard that explain how to categorize into security profiles? No*

   There are no documents or guidance found on how to categorize into relevant security profiles. A developer claims conformance to a security profile which is then evaluated for correctness.

2. *Does standard provide security profiles for cloud products/services specifically? No*

   CC (common criteria) contains a separate security profile of cloud products. Common criteria provide security control requirements for type of products called protection profiles (PP). The PP a product is suited to depends on type of technology in the product (e.g. Firewalls). Some other types pf protection profiles are Databases, Multi-function devices, operation systems etc. (Common Criteria, n.d.). From types of PP webpage (Common Criteria, n.d.), it is seen that while no cloud service related category is seen explicitly, types of IT technologies that are used in cloud services are provided. Some examples are file encryption protection profile in data protection category or Security Module Application for Electronic Recordkeeping Systems under other devices and systems category.

3. *Does standard specify requirements to follow in case product belongs to multiple profiles? Yes*

If product claims conformance to multiple PPs, it must fulfill requirements of each PP. A PP mentions if strict or demonstrable conformance is required. More information about types of conformance is provided in Introduction and general model document (Common Criteria, 2017).

4. *Are CSPs pursuing authorization responsible for choosing their product's security profile? Yes*
5. *If yes, does authorizing body validate the security profile? Yes*
6. *Does authorizing body check security profile in early stages of authorization? Yes*

A requirement by CC is for a developer to submit a conformance claim that explains rationale for conformance to a security profile type or PP. Developers use consistency with security problem of a PP and type of product as evidence to prove conformance.

CC divides assurance into scales of assurances from Evaluation Assurance Level EAL1-7. EAL 1 level of evaluation is the lowest assurance scale done where some assurance in correct operation of product is required, but threats to security are not viewed as serious. EAL 7 is the highest assurance scale used in cases where security threats are serious, and assets are of high value. All assurance scales between EAL1-7 evaluate conformance claim. Conformance claims are submitted initially in the process of certification along with product definition. (Common Criteria).

Privacy criteria

7. *Are privacy controls present? Yes*
   CC has privacy requirements divided into four categories under class name Privacy (Criteria, Common, 2017). Objective of privacy class is to protect a user's identity against discovery and misuse. Families of privacy class are anonymity, pseudonymity, unlinkability, unobservability.

Anonymity requires that a user be allowed to use a resource or a service without revealing the user's identity to other users/subjects.

Pseudonymity ensures that a user uses a resource or service without providing identity information but still be accountable. This is made possible by using an alias that is directly related to the identity of a user.

Unlinkability allows a user to make multiple uses of resources without others being able to link these uses back to the user.

Unobservability also intends to hide usage of a resource from other users. However, in this component this is done by hiding the use of resource or service, rather than hiding the user's identity.

8. *Is conformance strict for all businesses and types of service providers?* No

While preparing implementation documents for assessment, developers of product describe security problems and solutions in form of security objectives.

If privacy is identified as part of a security problem, then privacy requirements should be implemented by developer as part of solutions. To ensure that privacy requirements are identified and implemented correctly, assurance components are in place to verify this process. Also, if a security profile or PP has implemented privacy controls and developer is claiming conformance to such PP, privacy controls must be implemented (Criteria, Common, 2017).

9. *Are privacy controls derived from legislation, policies, procedures, and/or associated controls? Yes*

Privacy controls are described in CC requirements document (Criteria, Common, 2017). The structure of these controls is similar to structure of security requirements with a class name, family name, family behavior and related components. Privacy controls in CC are subject to similar implementation and assessment procedures as security requirements.

Security Requirements Criteria

10. *Are requirements divided into suitable categories? Yes*

CC divides security functional requirements into classes which are further divided into families and components. There are 11 classes each concerned with an aspect of IT security. Some classes are "Resource Utilization", "Security Management". The structure of a class consists of:

- **Class name**: unique and consists of a short name of three letters. For example, Class FCS identifies functional requirements for cryptographic support.
- **Class introduction**: describes the intent or approach of families under the class

A class is further divided into one or more "functional families". The structure of a functional family consists of: Description of a functional family provides family name, family behavior, component levelling, management and audit components.

Family name: gives information used to identify and categorize a function family. Family name has 7 characters in total. First three characters are identical to class name (three letters) followed by underscore followed by a short unique, three-character name of family. For example, for class FCS (cryptographic support class), two functional families named FCS_CKM (cryptographic key management) and FCS_COP (cryptographic operation) are present.

Family behavior: provides description that states security objective of the family and description of its functional requirements. For FCS_CKM (cryptographic key management) family, requirements for the following operations are provided: cryptographic key generation, cryptographic key distribution, cryptographic key access and cryptographic key destruction.

Component leveling: Once a family and its functional components are identified, component levelling describes each of those components in detail and their rationale. Any number of components can be included in PPs or target of evaluation (TOE) document. TOE is hardware/software being assessed. There are 4 components in FCS_CKM family as mentioned in paragraph above. FCS_CKM.1 describes cryptographic key generation, FCS_CKM.2 describes cryptographic key distribution, FCS_CKM.3 provides requirements for cryptographic key access and FCS_CKM.4 for and cryptographic key destruction.

Sometimes one component may be hierarchical to another if it offers more security. Hierarchical relationships are also indicated in this section. In FCS class there are no hierarchical components.

Management component: contains information on management activities that a product developer may consider for a given component. These are not mandatory requirements but meant as suggestions. For FCS_CKM family, no management activities are suggested.

Audit component: There is separate class called Audit Class cited in security requirements. If a developer is fulfilling requirements for audit class, then audit component section describes events that should be audited. Furthermore, this requirement mentions if minimal or detailed auditing of a security event is required. For FCS_CKM class, this requirement is minimal. This means that success or failure of security events that used the mechanism of cryptographic key management must be recorded.

11. *Is mapping of requirements between major standards available? No*

Requirements are not mapped between different standards. However, section E under "Bibliography" in Introduction And General Model document (Common Criteria, 2017) provides refers to some ISO/IEC standards and guidance documents for more information.

12. *Do standards acknowledge dependencies in its requirements? Yes*

Different type of dependencies such as dependencies between requirements, between assessment procedures or those between requirements and assessment procedures are mentioned in description of functional component. To fulfill requirements of a component, a developer also needs to fulfill requirement of the component's dependencies. The dependencies of a component are described in the component definition. For example, in FCS_CKM.1 cryptographic key generation component definition. dependencies are identified and their component identifiers are mentioned (FCS_CKM.2, FCS_CKM.4, FCS_COP.1). (Criteria, Common, 2017)

13. *Do standards provide requirements or ways to obtain requirements for layered architecture such as IaaS, PaaS, SaaS? Yes*

CC does not mention layered architecture such as IaaS, PaaS, SaaS as separate dependencies. Instead, it treats them as dependencies which are included in component definition of requirements and assurance.

14. *Do requirements reference other documents, publications, templates that can provide more clarity on requirements? Yes*

Security functional components document provides requirements established by CC. These requirements reference Introduction and General Model document (Common Criteria, 2017) as CC part 1 and security assurance component document as CC part 3. Common methodology for evaluation (CEM) is also referenced where appropriate (Common Criteria, 2009).

15. *Is physical infrastructure part of fulfilling requirements? Yes*

TSF physical protection (FPT_PHP) family of control calls for TSF to be designed so physical attacks to the system are detectable. It also requires that a TSF have features so it is resistant to attacks. Example of physical attacks are including but not limited to mechanical attack, radiation, changing the temperature.

Flexibility criteria

16. *Is standard applicable in more than one country? Yes*

    All signatories of CCRA (common criteria recognition arrangement), (Common Criteria, 2014), are government organizations that recognize products certified by CC. The list of CCRA participants can be found on (Common Criteria, n.d.). There are 31 member nations currently.

17. *Is this standard a strict requirement for industry/country of concern? No*

    The industry of concern to us is CSPs. While CC attestation alone is not directly recognized by an evaluation body, use of products certified with CC can be a favorable requirement to fulfill requirements for a standard that is directly associated with CSP. One such example are in FedRAMP high, low, medium baseline template requirements where acquisition process (SA-4) requirement is fulfilled by preferably using a product certified with CC (FedRAMP, 2018).

18. *Is this standard applicable in multiple industries? Yes*

    Products certified with CC can be used by many industries depending on type of technology a product employ.

19. *Does standard provide baseline configurations and allow tailored configurations to be layered on top? Yes*

    The standard allows protection profiles (PP) which act as baseline profiles or basic security requirements for a type of IT product. According to a PP, strict or demonstrable compliance to it is required. After identifying PP, developers pursuing certification implement security controls as mentioned in PP. Additional requirements can be added to requirements specified by a PP.

20. *Do requirements provide flexibility within security control requirements? Yes*

    Each security control provides flexibility using Iteration, assignment, selection and refinement options. They are described below briefly:

    Assignment operation allows the developer to assign a parameter in a security control. This parameter can be an unrestricted variable or have rules that narrow it down to specific range of values (Common Criteria, 2017).

    Selection operation allows the developer to select a parameter in a security control from choices given in the requirement.

    Iteration operation: It is possible to implement each component in many ways by applying assignments and selections on that component. Hence multiple iterations of the same component are possible.

    Refinement operation allows the developer to refine/change a parameter in a security control if change requirement is stricter than the original requirement.

21. *Is there room to provide alternate requirements? No*

    A product must show demonstrable or strict compliance with security controls as defined by PP.

22. *Is the standard scalable? Yes*

    CC certificates are authorized by certificate authorizing participants and certification/validation bodies present in each of participant's countries. The list of CBs is found here (Common Criteria, n.d.). As can be seen from this list, each member nation has 2 or more licensed labs that evaluate for certification/validation according to validation scheme set by CB according to security and assurance requirements described by CC (Common Criteria, 2014). Multiple levels of delegation and management make scalability possible. More labs can be certified if high volume of certifications are needed.

Transparency

23. *Does standard provide guidance on financial resources required for certification? No*

CC does not provide a general cost for certification. On investigating a licensed lab called Intertek evaluation labs in Canada, pre-evaluation consulting is offered where cost of the evaluation is discussed. (Intertek EWA Canada, n.d.)

24. *Does standard communicate progress/time to completion? No*

CC does not provide time for completion. Intertek labs discusses time to completion is decided during pre-evaluation consulting session (Intertek EWA Canada, n.d.). Other labs such as (Cygnacom Certification Services, 2018) also provide pre-assessment consulting.

Assessment Process Criteria

25. *Is evaluation delegated to third party assessment organizations (3PAO)? Yes*

An evaluation facility works with a authorizing body or certification body (CB) to conduct tests for assessments and manage and document these assessments.

26. *Is accreditation required for a 3PAO to operate as an assessment body? Yes*

There are three bodies that operate as 3PAOs during assessment. They are:

An evaluation facility as defined by CC is “An organization which carries out Evaluations, independently of the developers of the IT Products or Protection Profiles evaluated and usually on a commercial basis.” Such organization must be certified with ISO/IEC 17025 or similar. CC also sets additional requirements explained in Annex B3 under “Accreditation and Licensing of Evaluation Facilities” in Arrangement on the Recognition of CC certificates document (Common Criteria, 2014)

A certification/validation body (CB) is an organization tasked with ensuring the certification/validation scheme is carried out reliably. A CB oversees and record activities of an evaluation facility. Such organization must be certified with ISO/IEC 17025 or similar. CC also sets additional requirements explained in Annex C under “Requirements for Certification/Validation Body” in Arrangement on the Recognition of CC certificates document

Certificate Authorizing Participants/Members are sponsors of CBs. They further verify certificates passed by CBs but don’t perform any evaluation activities. A portion of signatories of Common Criteria Recognition Arrangement (CCRA) such as India, Canada, Japan are Certificate Authorizing Participants.

27. *Does standard provide criteria for evaluation of CSP? Yes*

Criteria for evaluation is discussed in detail in Report #2 (Gupta, Literature Survey: Cloud Security Evaluation Approaches, 2020). To summarize, CC provides assurance levels or a scale that a product can be evaluated against. It also provides assurance criteria for evaluation of new profiles and security target

(ST). Assurances are structurally similar to structure o requirements in that they are divided into class name subdivided into family, components and elements. About 9 classes of assurance are mentioned namely Class APE: Protection Profile evaluation, Class AVA: Vulnerability assessment

28. *Rate flexibility level given to 3PAOs to perform evaluation criteria or tests? Low, medium or high> Medium*

    3PAOs are offered medium flexibility which means that 3PAOs make their own tests, but tests must fulfill expectations and objectives of evaluation criteria provided by standard body. Evaluation bodies produce an evaluation scheme based on requirements given by CC. An evaluation scheme defined by CC as "The systematic organization of the functions of Evaluation and Certification/Validation under the authority of a CB in order to ensure that high standards of competence and impartiality are maintained, and that consistency is achieved."–(Common Criteria, 2014). There are processes in place that ensure that evaluation scheme adheres to evaluation criteria given by CC.

29. *Is clear distinction provided between responsibilities of developer and authorizing body about division of responsibility between developers and assessors? Yes*

    Under each class of evaluation requirement, which are further divided into components, the component description delegates requirements of the class to developer and assessor. For example, in component ASE_INT (Security Target introduction) in class ASE (Security Target Evaluation), component ASE_INT.1.1D requires that "The developer shall provide an ST introduction" (Common Criteria, 2017). The D character ASE_INT.1.1D indicates delegation of responsibility of implementing this requirement to developer. Further down, evaluator action elements are mentioned. In ASE_INT.1.1E, E signifies allocation of responsibility to evaluator.

30. *Does assessment procedure explain limitations? Yes*

    In section A.6.4 under Assumptions, CC describes assumptions that evaluators assume to be true and hence do not evaluate for them. These assumptions are made with respect to operational environment of a product. Physical, personnel, connectivity aspects are part of these assumptions. For example, it is assumed that Target of Evaluation (TOE) is placed in a room that has minimum electromagnetic emanations. If security control is not implemented because some of these assumptions are not true, then requirements may be tailored.

Reassessment and Continuous Monitoring

31. *Is reassessment mandatory? No*
    Reassessment or reevaluation is not mandatory if changes are made to a product don't adversely affect the assurance baseline. The developer must demonstrate that no real change has been made to a TOE, IT environment and/or development environment. Reevaluation is done if developer indicates that there are major changes to pre-certified product or does not provide convincing evidence of otherwise. Reevaluation is done by same 3PAO that performed initial evaluation. It is assumed that the developer can be trusted to provide accurate detail of changes to evaluator. In case of new vulnerabilities or change in threat environment, re-evaluation is required (Common Criteria, 2012).

32. *Is continuous assessment frequency interval and related procedure decided between product developer and assessing body during evaluation phase of certification process? No*

A fixed interval is not necessarily decided as maintenance or relation process is only triggered if there are minor (maintenance) or major (reevaluation) changes made to a TOE. This procedure is decided beforehand and standardized by CC in Assurance Continuity Requirements document (Common Criteria, 2012).

33. *Does standard require fixed frequency interval for reassessment? No*
34. *If no, is frequency for reassessment flexible? Yes*

As mentioned, reevaluation only happens if there is a change to TOE and no fixed frequency interval has been mentioned. Therefore, frequency of reassessment will become flexible.

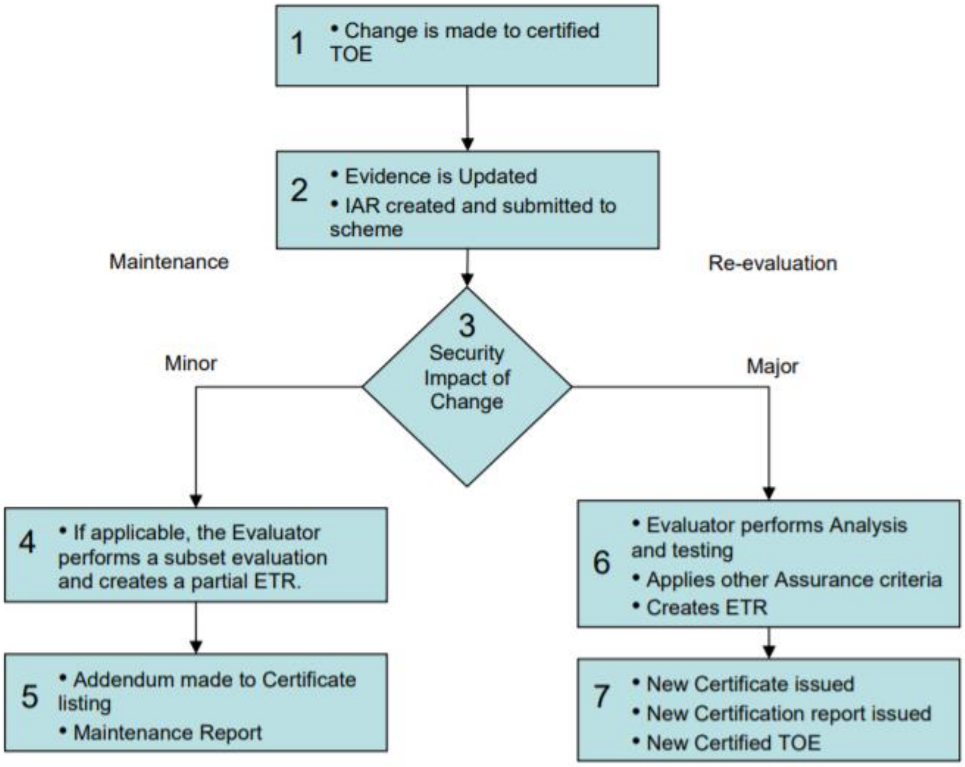
1
• Change is made to certified TOE
2
• Evidence is Updated
• IAR created and submitted to scheme
Maintenance
Re-evaluation
3
Security Impact of Change
Minor
Major
4
• If applicable, the Evaluator performs a subset evaluation and creates a partial ETR.
5
• Addendum made to Certificate listing
• Maintenance Report
6
• Evaluator performs Analysis and testing
• Applies other Assurance criteria
• Creates ETR
7
• New Certificate issued
• New Certification report issued
• New Certified TOE

Figure 1: Assurance Continuity for CC

35. *Are bodies conducting reassessment mentioned in standard documents? Yes*

(Common Criteria, 2012) CC assumes that developer will submit IAR report to the same evaluation authority that provided original certification during regular maintenance. However, the document is not clear about whether this relationship is mandatory.

36. *Are procedures in place to address new vulnerabilities/changes? Yes*

A reevaluation is necessary to address new vulnerabilities/changes. Class AVA (vulnerability assessment) is evaluation class that addresses vulnerabilities that may be exploited during development or operation of product. Its objective is to have the evaluator perform tests including penetration testing to obtain information about these vulnerabilities. This leads to a vulnerability analysis report that is shared with developer. If there is a change in vulnerability analysis report, it must be documented by developer and shared with evaluator for reevaluation (Common Criteria, 2017).

37. *Are changes to product classified according to impact of change? Yes*
38. *If yes, are each of these classifications described clearly in reassessment or standard documents? Yes*

Changes are classified as minor or major changes. More guidance on classification of changes is given in Assurance Continuity document (Common Criteria, 2012). For example, some major changes are changes to claimed assurance or functional requirements. Some minor changes are changes IT environment that do not change certified TOE or changes in grammar or formatting.

39. *Is subset evaluation done in case changes are minor? Yes*

Only a subset of controls is reevaluated when minor changes occur. An affiliated evaluation facility identifies assurance criteria that are affected by such changes and reevaluate those components.

40. *Do standard documents mention requirements that are not reassessed? Yes*

Requirements that are not affected by changes to product are not reassessed. Evaluation results from previous reassessment are used to verify compliance.

41. *Does standard allow 3PAOs to be reassessed or monitored continuously? Yes*

Periodic assessment of complaint CBs in required at least every five years. The management committee of CC asks qualified participants to carry out a periodic assessment.

FedRAMP

Security Profile Criteria

1. *Are documents/templates provided by standard that explain how to categorize into security profiles? Yes*

FedRAMP asks federal departments to refer to Federal Information Processing Standards (FIPS) PUB 199 documents. FIPS provides a standard for security categorization of all federal information and information systems with exceptions specified (National Institute of Standards and Technology , 2004). Categorization is based on potential impact to confidentiality, integrity and availability of an organization’s resources and information in case of security breach. Vulnerability and threat information are used for assessing impact as well. Impact is scaled to low, moderate and high. Some examples/use cases are provided for each category. Report #2 (Gupta, Literature Survey: Cloud Security Evaluation Approaches, 2020)describes them in detail.

2. *Does standard provide security profiles for cloud products/services specifically? No*

While FedRAMP standard applies to CSPs wanting to provide services to federal government, security profiles for a CSP is not separate from ones used for all information and information systems.

3. *Does standard specify requirements to follow in case product belongs to multiple profiles? Yes*

For different information types and functions in a system with each belonging to low, medium or high types of security profiles, the system on a whole should be assigned the highest scale. For example, if payroll information on a system has moderate confidentiality and administrative information has low confidentiality, then the entire system must be categorized with moderate confidentiality. (National Institute of Standards and Technology , 2004)

4. *Are CSPs pursuing authorization responsible for choosing their product's security profile? Yes*
5. *If yes, does authorizing body validate the security profile? Yes*
6. *Does authorizing body check security profile in early stages of authorization? Yes*

In the System Security Plan (SSP) submitted by a CSP, along with explaining a system's security objective, it is required to identify conformance with low, medium or high impact. This document is reviewed and approved by assessing agency before assessment process begins. (FedRAMP, n.d.)

Privacy criteria

7. *Are privacy controls present? Yes*

There are 8 privacy control families as listed below. The objective is to protect individual information that is collected, used, maintained, shared and disposed by programs and information systems of the government (National Institute of Standards and Technology, 2013).

- Authority and Purpose
- Accountability, Audit, and Risk Management
- Data Quality and Integrity
- Data Minimization and Retention
- Individual Participation and Redress
- Security
- Transparency
- Use Limitation

8. *Is conformance strict for all businesses and types of service providers? No*

Privacy controls are implemented for businesses with Personally Identifiable Information units. PII is defined by OMB memorandum 07-16 as: "Information which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.)." (EXECUTIVE OFFICE OF THE PRESIDENT,Office of Managment and Budget Washington, 2007)

FedRAMP publishes a Privacy Impact Assessment (PIA) template for organizations to evaluate if the CSP uses and stores PIIs (FedRAMP, 2017). Information about aspects of PIIs such as sources, purpose, access safeguards liabilities etc. is collected.

9. *Are privacy controls derived from legislation, policies, procedures, and/or associated controls?*

Privacy controls are based on Fair Information Practice Principles (FIPPs) embodied in the Privacy Act of 1974, Section 208 of the E-Government Act of 2002, and Office of Management and Budget (OMB) policies (National Institute of Standards and Technology, 2013).

Security Requirements Criteria

10. Are requirements divided into suitable categories? Yes

    FedRAMP requirements are derived from NIST SP 800-53 Revision 4 security controls. Controls presented by NIST SP 800-53 are tailored for cloud computing systems. To start, requirements are categorized into low, moderate or high baseline requirements according to a system's analysis of impact on services in case of security breach. Impact analysis process is described in more detail in (Gupta, Literature Survey: Cloud Security Evaluation Approaches, 2020). Overall, there are 18 families. Each family is identified with a two-character name. For example, AU identifies Audit and Accountability. Each family is further divided into subcomponents related to main family class. Each subcomponent is serially numbered. For example, AU-1 (Audit And Accountability Policy And Procedures), AU-3 (content of audit records) are subcomponents of AU family. These subcomponents consist of:

    Control section: describes security-related activities or actions to be implemented. More than one control definitions are numbered a),b) and so on.

    Supplemental Guidance: optional information provided to apply when implementing security control

    Control Enhancement: provides information in form of statements to increase capability of security control or add functionality to control section. They are not mandatory but can be implemented optional to a base control. Control enhancements are numbered sequentially. For example, AU-3(1) identifies Additional Audit Information as a control enhancement, AU-3(2) identifies Centralized Management of Planned Audit Record Content as another control enhancement.

    References section refers to applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines (e.g., OMB Circulars/Memoranda, Homeland Security Presidential Directives, FIPS Publications, and NIST Special Publications) that are relevant to a particular security control (National Institute of Standards and Technology, 2013).

11. *Is mapping of requirements between major standards available?*

    FedRAMP directly does not provide mapping between its requirements to other important standards such as those of ISO/IEC. However, NIST maps security controls to ISO/IEC 27001 and common criteria. Since FedRAMP derives heavily from NIST security controls, mapping of NIST controls between international standards can be useful for CSPs pursuing FedRAMP authorization. The intention of mapping between NIST Special Publication 800-53 and ISO/IEC 27001 is to show equivalent security controls so corresponding security posture is obtained. Details on methodology used for mapping and examples to showcase intent is found in Appendix H of NIST Special Publication 800-39. Mapping between CC and NIST Special Publication 800-53 controls is called "informal" and does not serve to determine if requirements of CC may be satisfied by implementing controls of NIST.

12. *Do standards acknowledge dependencies in its requirements? Yes*

    There are families of security requirements that need developers to acknowledge existing dependencies. For example, under planning (PL) family, alongside subcomponent (PL-8) information security architecture (PL-8) it is essential that dependencies of the architecture of external services must be described. There is also a requirement (SC-3) that asks for modular software design to reduce coupling and hence dependency.

13. *Do standards provide requirements or ways to obtain requirements for layered architecture such as IaaS, PaaS, SaaS? Yes*

    FedRAMP says that each layer of IaaS, PaaS, SaaS must be evaluated separately. If one of the layers is already authorized, it is possible to tailor security controls for layers atop (National Institute of Standards and Technology, 2013). One such tailored baseline is provided for low impact SaaS type profile (FedRAMP, 2018). FedRAMP SSP template will allow a CSP to record controls inherited from a system. However, description of controls is only needed for requirements that are implemented by developer (FedRAMP, 2018).

14. *Do requirements reference other documents, publications, templates that can provide more clarity on requirements? Yes*

    In column H of security controls baseline template document provided by FedRAMP, additional information is provided under guidance section (FedRAMP, 2018).Also since most of FedRAMP's controls can be found in NIST Special Publication 800-53 where references to each security requirement is explicitly stated as a separate section in component description (National Institute of Standards and Technology, 2013).

15. *Is physical infrastructure part of fulfilling requirements? Yes*

    Under physical and environmental protection (PE) family of requirements, it is required to develop policy for physical and environmental protection, implement physical access control, monitoring physical access etc. (National Institute of Standards and Technology, 2013)

Flexibility

16. *Is this standard applicable in more than one country? No*

    According to OMB memorandum introduced on December 98, 2011 (Executive Office of the President, Office of Management and Budget, 2011), FedRAMP is developed to be used for information systems used by executive departments and agencies.

17. *Is this standard a strict requirement for an industry/country? yes*

    CSPs, commercial or noncommercial, who want to supply cloud services to the government, must be certified with FedRAMP.

18. *Is this standard applicable in multiple industries? No*

    This standard cannot be used to show validate security posture for any industry other than government of US.

19. *Does standard provide baseline configurations and allow tailored configurations to be layered on top? Yes*

    Firstly, an organization identifies security profile according to standards according to FIPS PUB 199 (National Institute of Standards and Technology , 2004) and communicated required security controls to CSPs. It can select compensating security controls if it is not possible to implement certain controls. Such tailoring of requirements must be approved by a partnered 3PAO in an organization's initial SSP before they are implemented.

Sometimes there may be a need to implement a tailored set security controls for a community or several systems. (National Institute of Standards and Technology, 2013) In that case, FedRAMP allows overlays, a fully specified set of security controls, control enhancements and supplemental guidance by applying tailoring process. One such system is a Low Impact-SaaS baseline (FedRAMP, 2018). FedRAMP controls are tailored from NIST (FedRAMP, 2018).

20. *Do requirements provide flexibility within security control requirements? Yes*

    Like CC, selection and assignment statements are present in some security controls to provide flexibility (National Institute of Standards and Technology, 2013).

21. *Is there room to provide alternate requirements? Yes*

    Assumptions about operational environment of systems are made such as information systems being in physical facilities, systems existing in networked environment that influenced security controls of baselines. If these assumptions are not fulfilled Itis possible to provide alternate requirements (National Institute of Standards and Technology, 2013).

22. *Is the standard scalable? No*

    During pre-authorization stage, CSP interacts with FedRAMP Program Management Office (PMO) to obtain consultative help. This can be strenuous on PMO's resources as more services pursue authorization. Additionally, alternate route of assessment is available through JAB authorization. JAB consists of chief information officers from designated departments (Executive Office of the President, Office of Management and Budget, 2011). JAB process can authorize limited number of CSPs a year according to priority (FedRAMP, n.d.). According to (FedRAMP Fast Forward Industry Advocacy Group, 2016) , scalability is cited as a significant problem.

Transparency

23. *Does standard provide guidance on financial resources required for certification? No*

    FedRAMP does not provide this information.

24. *Does standard communicate progress/time to completion? No*

    No process of communicating progress is found. In SAP document submitted by 3PAO and shared with CSP pursuing certification, FedRAMP requires 3PAO to present a schedule for assessment process. (FedRAMP, n.d.) explains JAB authorization process where rough timeline to complete each process is provided.

Assessment Process Criteria

25. *Is evaluation delegated to third party assessment organizations (3PAO)? Yes*

    3PAOs are responsible for assessing requirements implemented by CSPs initially and periodically. A CSP partners with a 3PAO initially followed by engagement with FedRAMP Program Management Office (PMO) to receive guidance on strategy of implementation and evaluation.

26. *Is accreditation required for a 3PAO to operate as an assessment body?* Yes

Organizations interested in becoming accredited FedRAMP 3PAOs must be reviewed by the American Association for Laboratory Accreditation (A2LA), which follows ISO/IEC 17020:2012 Requirements for the Operation of Various Types of Bodies Performing Inspection (FedRAMP, n.d.). Acceptance of A2LA accreditation for a 3PAO is subject to final approval by the FedRAMP PMO. FedRAMP and A2LA work together to have their own set of requirements besides ISO/IEC for quality assurance. More information about this can be found in R311 -Specific Requirements: FedRAMP(A2LA, 2019). In summary, the document states requirements for 3PAO applicants to identify discrepancies within a test security plan to show knowledge of FedRAMP assessment framework. There are also requirements for personnel in a 3PAO assessment team to include a senior representative, penetration tester and quality management representative. Personnel must display knowledge FedRAMP management and laws and regulation.

27. *Does standard provide criteria for evaluation of CSPs?*

Criteria for evaluation is discussed in detail in Report #2. FedRAMP's Security Assessment Framework (FedRAMP, 2017) consists of four processes of: Document, Assess, Authorize, and Monitor. These align with the NIST Risk Management Framework (RMF) (NIST, 2018). To summarize, FedRAMP provides evaluation criteria through use of templates it provides to CSPs to fill with information as they prepare for certification. Through this template, called System Security Plan (SSP) (FedRAMP, 2018), it will ask CSP to document implemented requirements in format dictated by FedRAMP. Additionally, assessment bodies use a Security Assessment Plan (SAP) (FedRAMP, 2017) (FedRAMP, 2017) and Security Assessment Requirement (SAR) template to perform and document tests, risk analysis, corrective actions. The basis for these templates can be assumed to be criteria for evaluation. All these templates provide such reference to basis under "Applicable standards and guidance section/laws and regulation" from where these templates were derived.

28. *Rate flexibility level given to third-party assessors to perform evaluation criteria or tests? Low, medium or high*

Flexibility is rated Medium as guidance for assessment to a 3PAO is provided in the form of SAP (FedRAMP, 2017). SAP includes sections where scope of assessment, assumptions, methodology, testing performed using automated tools and manual tools is recorded by 3PAO. FedRAMP Assessment Framework document (FedRAMP, 2017) describes assessment from initial documentation phase where security controls are implemented followed by assessment and authorization phase to monitoring phase (FedRAMP, 2017). A SAP test case procedures template (FedRAMP, 2017) allows for recording of tests and results obtained for low, medium, high baseline configurations separately. For some security controls, mechanisms to test are mentioned. Type of results to be recorded are risk exposure level, impact level etc.

29. *Is clear distinction provided between responsibilities of developer and authorizing body? Yes*

Security Assessment Framework document (FedRAMP, 2017) highlights process of evaluation and is discussed in detail is report #2. FedRAMP's website dedicates separate webpages to responsibilities of CSPs and 3PAOs during authorization process of FedRAMP (FedRAMP, n.d.) (FedRAMP, n.d.). To summarize, developers implement security controls according to security control catalogue for suitable baseline (low, medium, high) followed by documenting in an SSP using SSP template provided by FedRAMP. SSP describes how an implementation fulfills security control, roles and responsibilities and expected behavior of users of system. This document is reviewed with a 3PAO and upon satisfaction, initiates the certification process. An assessor is responsible for completing a SAP document resources to be assessed are recorded. These include hardware components, software functions and physical facilities.

30. *Does assessment procedure explain limitations? No*

No limitation was found to be described by FedRAMP in their assessment process.

Reassessment and Continuous Monitoring

31. *Is reassessment mandatory? No*

FedRAMP's continuous monitoring process is based on NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organization. Security control mechanisms are monitored periodically by 3PAO. In case of significant change, a reassessment process is initiated.

32. *Is continuous assessment frequency interval and related procedure decided between product developer and assessing body during evaluation phase of certification process? Yes*

A Continuous Monitoring Program/Plan is established between assessing body and CSP where 3PAOs assess subset of security controls at least annually. Some controls may be monitored and reassessed more frequently. An authorizing official body consists of members of agency that is using the CSP's system. It oversees continuous monitoring activities of CSP and offer consultation on security controls to be reassessed.

33. *Does standard require fixed frequency interval for reassessment? No*
34. *Is frequency for reassessment flexible? Yes*

Frequency interval is flexible provided assessment is done at least annually if evaluation is done by 3PAO. In case another authorization route is taken, such as choosing to get authorized by Joint Authorization Board (JAB), minimal required frequency for reevaluation is not clear. Table 2 in "FedRAMP Continuous Monitoring Strategy Guide" describes reassessment process for each control and suggested frequency for reevaluation. Actual intervals are decided in consultation with AO. (FedRAMP, 2018)

35. *Are bodies conducting reassessment mentioned in standard documents? Yes*

Under continuous monitoring roles and responsibilities, details are provided about different bodies and their role in monitoring or reevaluation process. Question # (insert) mentions AOs and their responsibility. Besides them, FedRAMP JAB manages reevaluation process if P-ATO (write full form) route of certification is taken. FedRAMP program management office (PMO) acts as liaison between JAB and CSPs. 3PAOs are responsible for assessing and sending reports to AOs.

36. *Are procedures in place to address new vulnerabilities/changes? Yes*

All changes including vulnerabilities are recorded in configuration management plan managed by developer. During annual assessment by evaluator, impact of these changes is recorded by evaluator and shared with AO. In consultation with evaluator, AO decided which controls should be reevaluated.

37. *Are changes to product classified according to impact of change? Yes*
38. *Are each of these classifications described clearly in reassessment or standard documents? No*

Changes are classified into minor or significant changes. Standard documents do not provide guidance on difference between significant and minor changes. A developer must perform security impact analysis as part of its configuration management plan. To classify impact of change as being minor or significant, FedRAMP recommends 3PAO consult with AO.

39. *Is subset evaluation done in case changes are minor? Yes*

    Any minor or major change is identified by developer and made known to AO. AO selects controls that need to be reassessed and assigns them to 3PAO.

40. *Do standard documents mention requirements that are not reassessed? Yes*

    Since only controls decided by AO are reassessed depending on impact of change on security of controls, there are several changes that are not reassessed

41. *Does standard allow 3PAOs to be reassessed or monitored continuously? Yes*

    A full reassessment of a 3PAO happens after every 2 years managed by A2LA. The reassessment is done on the same parameters as original assessment of a 3PAO. (FedRAMP, 2017)

Information Technology Security Guidance (ITSG-33)

Security profile criteria

1. *Are documents/templates provided by standard that explain how to categorize into security profiles? Yes*

   Annex 4 of IT Security Risk Management: A Lifecycle Approach includes a “series of suggested control profiles” (Communication Security Establishment Canada, 2012).. In Annex 4, profile 1 – Protected B, medium integrity, medium availability and profile 3-Secret, medium integrity and medium availability (Communication Security Establishment Canada, 2012). In description of security profiles, business, technical and threat context with examples and use cases are mentioned which are useful in classifying into profiles.

2. *Does standard provide security profiles for cloud products/services specifically? No*

   Information Technology Security Guidance (ITSG-33) provides a framework of IT risk management for any IT project plan including cloud services. The document acknowledges that security profiles are designed after Communications Security Establishment (CSE)’s careful selection from NIST, FedRAMP, ISO 27000 standards and to meet Treasury Board of Canada Secretariat (TBS) security objectives.

3. *Does standard specify requirements to follow in case product belongs to multiple profiles? No*

   The standard provides limited information and refers to FedRAMP guidelines for guidance.

4. *Are CSPs pursuing authorization responsible for choosing their product’s security profile? No*
5. *Does authorizing body validate the security profile? Yes*
6. *Does authorizing body check security profile in early stages of authorization? Yes*

   Overview section of (Canadian Centre for Cyber Security (CCCS), 2018) mentions that security profiles are chosen by the GC department looking to employ a CSP’s services. Chosen profile is communicated to a

CSP which implements baseline controls along with GC. Selected security profile is assessed by CCCS assessment team during early phase of assessment process.

Privacy criteria

7. *Are privacy controls present? No*

   No privacy controls or families are mentioned explicitly in security control catalogue of ITSG-33. Under planning (PL) family, privacy impact assessment (PL-5) is mentioned as “now withdrawn”. Some controls such as System Use Notification (AC-8), Publicly Accessible Content (AC-22), Access Control Decisions (AC-24), Information Leakage (PE-19) have privacy components.

8. *Is conformance strict for all businesses and types of service providers? No*

   Since no privacy controls are present, question about conformance does not arise. Controls that require some component of privacy as mentioned above are flexible to apply according to identified security profile.

9. *Are privacy controls derived from legislation, policies, procedures, and/or associated controls? No*

   This question is not applicable as privacy controls are not present.

Security Requirements Criteria

10. *Are requirements divided into suitable categories? Yes*

    In ITSG-33, security control requirements are divided into seventeen classes concerning technical security controls, operational security controls and management security controls. These controls are further divided into families and subcomponents. (CCCS, 2018)The structure of security catalogue is same as that of FedRAMP (FedRAMP, 2018) and NIST 800-54 (National Institute of Standards and Technology, 2013).

11. *Is mapping of requirements between major standards available? Yes*

    Under “ Additional References” section 4.1 of ITSG-33 security control catalogue (CCCS, 2018), each control has been linked to third-party (non-GC) publications on information security and security controls.

12. *Do standards acknowledge dependencies in its requirements? Yes*

    Like FedRAMP, ITSG-33 also acknowledges dependencies within certain security controls (PL-8, SC-3)

13. *Do standards provide requirements or ways to obtain requirements for layered architecture such as IaaS, PaaS, SaaS? No*

    No mention IaaS, PaaS, SaaS or layered architecture is found.

14. *Do requirements reference other documents, publications, templates that can provide more clarity on requirements? Yes*

    In section 4 References in ITSG-33 security catalogue, each security control is referenced to a publication, legislation and/or associated control. For example, PL-2 control can be referenced from Treasury Board Secretariat of Canada. Information Technology Security – Audit Guide. September 1995. (CCCS, 2018)

15. *Is physical infrastructure part of fulfilling requirements?* yes

Audit requirements (AU-6) asks that an audit is maintained for physical access, temperature and humidity, and other defined physical controls. Under physical and environmental protection (PE) family of requirements, it is required to develop policy for physical and environmental protection, implement physical access control, monitoring physical access etc.

Flexibility

16. *Is this standard applicable in more than one country? No*

    Compliance with this standard is only recognized in Canada.

17. *Is this standard a strict requirement for an industry/country? Yes*

    CSPs wanting to supply cloud services to GC must be approved by CCCS assessment process

18. *Is this standard applicable in multiple industries? No*

    CCCS assessment cannot be used to show validate security posture for any industry other than government of Canada.

19. *Does standard provide baseline configurations and allow tailored configurations to be layered on top? Yes*

    Overview section of (Canadian Centre for Cyber Security (CCCS), 2018) describes security profiles to be baseline requirements that need to be tailored according to needs of client. Under description of each profile (Annex 4) from (Canadian Centre for Cyber Security (CCCS), 2018) provides tailoring guidance. Tailoring security controls to meet organizational needs is a requirement under security engineering control (SA-8).

20. *Do requirements provide flexibility within security control requirements Yes*

    Assignment and selection operations are provided in security controls as well (CCCS, 2018).

21. *Is there room to provide alternate requirements? Yes*

    With proper rationale provided in attestation documents, it is possible to provide alternate requirements. CCCS assessment team works with CSP throughout assessment process to review these documents.

22. *Is the standard scalable? No*

    All phases of assessment are done by CCCS. Delegation and automation is limited which hinders scalability.

Transparency

23. *Does standard provide guidance on financial resources required for certification? No*

    This information is not provided.

24. *Does standard communicate progress/time to completion? No*

    This information is not provided.

Assessment Process Criteria

25. *Is evaluation delegated to third-party assessors(3PAO)? No*

    Assessment are done by security experts and evaluators at Canadian Centre for Cyber Security (CCCS), a unit under Communications Security Establishment (CSE) agency of Canada, that monitors threats and organizes national response to any cyber security incident. Additionally, evaluation done by CCCS rely on attestations done by other international standards.

26. *Is accreditation required for a 3PAO to operate as an assessment body? No*

    No such information has been mentioned.

27. *Does standard provide criteria for evaluation? Yes*

    Attestations from other international standards along with independent evaluation by CCCS personnel is used as evidence for providing certification. No separate criteria, independent of other standards' criteria is found. Recognized international standards are System Security Plans (SSP) produced for FedRAMP, AICPA SOC 2 Type II reports, ISO/IEC 27001 reports, ISO/IEC 27017 reports.

28. *Rate flexibility level given to third-party assessors to perform evaluation criteria or tests? Low, medium or high*

    High flexibility is provided. CCCS is free to form their own evaluation criteria.

29. *Is clear distinction provided between responsibilities of developer and authorizing body about division of responsibility between developers and assessors? No*

    There is no clear distinction provided.

30. *Does assessment procedure explain limitations? Yes*

    (CCCS, 2018) explains following limitations during assessment:

    - Profiles identified with high impact levels with confidentiality, availability or integrity are not assessed because providing these services using cloud is not pursued.
    - Privacy requirements are restricted to protection of confidentiality, integrity and availability of GC information.
    - 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.).

Reassessment and Continuous Monitoring

31. *Is reassessment mandatory? No*

    According to CCCS assessment framework document (CCCS, 2018) , Government of Canada (GC) client continuously monitors the security posture of the cloud-based GC. No guidance about reassessment process is found. There is a brief indication that some public cloud services need to be reevaluated periodically. No further description is provided.

32. *Is continuous assessment frequency interval and related procedure decided between product developer and assessing body during evaluation phase of certification process? Yes*

After fourth and final phase of assessment the CCCS evaluation team makes recommendations to GC client about how often their implemented controls should be reassessed.

33. *Does standard require fixed frequency interval for reassessment? No*
34. *Is frequency for reassessment flexible? Yes*

Frequency interval of reassessment is flexible depending on recommendation of CCCS assessment team

35. *Are bodies conducting reassessment mentioned in standard documents? Yes*

CCCS is responsible for responding to GC client reassessment request. Further information about scope of their reassessment is lacking

36. *Are procedures in place to address new vulnerabilities/changes? No*

Information not available

37. *Are changes to product classified according to degree or impact of change?*
38. *If yes, are each of these classifications described clearly in reassessment or standard documents?*

Information not available. No, change classification is not described in standard documents.

39. *Is subset evaluation done in case changes are minor?*

Information not available.

40. *Do standard documents mention requirements that are not reassessed? No*
41. *Does standard allow 3PAOs to be reassessed or monitored continuously? No*

This question is not applicable to CCCS assessment as compliance testing is not done by 3PAOs but CCCS directly.

E. Comparison between standards

Following section summarizes main points of evaluation from section D for tested standards and compares between them. Table 1 presents results in tabular form.

Security Profile Criteria

1. *Are documents/templates provided by standard that explain how to categorize into security profiles*

CC does not provide documents or template that allows a product developer pursuing compliance to decide a suitable security profile and instead relies on a developer's best judgement. However, since PPs are types of IT products, there may be reason to believe that a developer does not require guidance in this regard. For example, developer of Minute Gap v18.5 Firewall can claim conformance to the firewall PP. FedRAMP references FIPS PUB 199 that provides guidance with examples and use cases. CCCS does not provide documentation either but redirects businesses to refer to FIPS (National Institute of Standards and Technology , 2004)and NIST (National Institute of Standards and Technology, 2013) as its security control catalog is derived from them. CCCS provides guidance about classification in description of specific security profiles. Unlike FedRAMP, it does not provide this information in a separate document of its own.

2. *Does standard provide security profiles for cloud products/services specifically?*

CC, FedRAMP and CCCS do not security profiles for cloud products/services specifically. Security profiles provided by FedRAMP and CCCS are derived from same legislations, laws, regulations and/or associated controls.

3. *Does standard specify requirements to follow in case product belongs to multiple profiles?*

   CC mentions chain type of conformance where two different PP types can be conformed to by fulfilling requirements of all PPs. Since security profiles in FedRAMP are based on impact analysis, product that conforms with multiple levels of impact is required to identify with highest watermark. CCCS provides limited information and refers to FedRAMP guidelines for guidance.

4. *Are CSPs pursuing authorization responsible for choosing their product's security profile?*
5. *If yes, does authorizing body validate the security profile?*
6. *Does authorizing body check security profile in early stages of authorization?*

   In CC, developers are responsible for submitting a conformance claim to assurance party. This conformance claim is submitted and evaluated initially in the process. Assessing parties at FedRAMP and CCCS also validate security profile in early stages of authorization.

Privacy criteria

7. *Are privacy controls present?*

   Privacy controls in CC are categorized into families of anonymity, pseudonymity, unlikability, unobservability. FedRAMP identifies 8 families of privacy controls. In ITSG-33, separate families of privacy control are not present. Privacy is enacted intro security controls belonging to access control families. The controls are the same controls present in FedRAMP.

8. *Is conformance strict for all businesses and types of service providers?*

   CC only required privacy controls to be implemented if privacy is seen as a security problem or if privacy controls are implemented in the PP to which the product claims conformance. FedRAMP only requires businesses with PII to implement privacy controls. There are assessment procedures verify that privacy is identified, and controls are implemented reliably. Unlike CC where product conforming to a PP that implements privacy controls must apply privacy also, belonging to a type security profile (low, medium or high baseline) does not necessitate implementing privacy controls in FedRAMP. For a GC department, since no privacy controls are present, question about conformance does not arise.

9. *Are privacy controls derived from legislation, policies, procedures, and/or associated controls?*

   FedRAMP and CC 's privacy controls are derived from legislation, policies, procedures, and/or associated controls.

Security requirements criteria

10. *Are requirements divided into suitable categories?*

    In CC, security requirements are divided into classes which are further divided into families and related components. Each class and related family are given a unique name to make identification easier. CC contains 11 classes, while FedRAMP consists of 18 families. Classes in CC perform the same function as those of families in FedRAMP in that each class or family deals with a unique aspect of security. Both classes and families in CC and FedRAMP respectively are identified with a unique name (three-character in CC and two-character in FedRAMP). In CC, a class is divided into families, each of which are given a 7-character unique name. In FedRAMP families are divided into subcomponents. Subcomponents in FedRAMP are numbered serially instead of being assigned unique characters.

As detailed in (name question), each family of CC security requirement identifies components described in component levelling section. These operations supplement implementation of a family and perform similar function as control enhancements in FedRAMP. In both standards, they are optional to apply and are identified sequentially alongside family name.

In ISTG-33, there are seventeen families all of which are like FedRAMP and NIST except program management class which is not present in ITSG-33 security catalogue. There were no other differences found.

11. *Is mapping of requirements between major standards available?*

    CC does not provide mapping between security requirements of security standards. To map controls in FedRAMP, mapping between NIST Special Publication 800-53, CC and ISO/IEC 27001 are available. However, use and methodology of mapping must be perused to determine consistency with reader's purpose. ITSG-33 also provides mapping between controls. Here equivalency between security controls can be established easily as security controls in ITSG-33 are found directly in NIST documents.

12. *Do standards acknowledge dependencies in its requirements?*

    CC provides dependencies as an explicit section under component description. FedRAMP does not acknowledge dependencies explicitly into a designated section but mentions dependencies, if any, in component description. ITSG-33 recognizes dependencies like FedRAMP.

13. *Do standards provide requirements or ways to obtain requirements for layered architecture such as IaaS, PaaS, SaaS?*

    CC does not provide requirements specifically while FedRAMP acknowledges layer dependencies and multi-tenancy in IaaS, PaaS, SaaS. This is because CC is a high level abstraction of security objectives and therefore, includes IaaS, PaaS, SaaS with dependencies. However, FedRAMP focuses on cloud technology products. ITSG-33 does not layered architecture.

14. *Do requirements reference other documents, publications, templates that can provide more clarity on requirements?*

    Requirements provided by CC are fairly independent in that they are not derived from existing legislation or publication but have been produced by experts in field of security with the intention to have a common criteria to evaluate security in IT products independent of other international standards. Therefore, requirements in CC will be referenced to other publications provided by CC itself. But CC provides references to some international standards for supplemental information. FedRAMP provides reference in component description of each control or requirement. ITSG-33 provides references in a handy table where each control is referenced.

15. *Is physical infrastructure part of fulfilling requirements?*

CC lists TSF physical protection (FPT_PHP) family of requirement to protect functionality against physical attacks. FedRAMP and ITSG-33 require consideration for physical security in audit (AU-3) family and physical and environmental protection (PE) family. Both FedRAMP and CC base requirements for physical controls on assumptions about operational environment that are mentioned in standard document.

Flexibility Criteria

16. *Is standard applicable in more than one country? No*

    It is applicable in 31 member nations that identify as signatories of CCRA. Compliance with FedRAMP regulations and ITSG-33 is recognized in government of US and GC respectively.

17. *Is this standard a strict requirement for industry/country of concern?*

    CC is not a requirement, only preferred. FedRAMP is a mandatory requirement for CSPs wanting to supply cloud services to the government of United States of America. Compliance with ITSG-33 is requirement for CSPs wanting to supply cloud services to the government of Canada.

18. *Is this standard applicable in multiple industries?*

    Products certified with CC can be used by many industries depending on type of technology a product employs. FedRAMP cannot be used to show validate security posture for any industry other than government of US.

19. *Does standard provide baseline configurations and allow tailored configurations to be layered on top?*

    CC allows security profiles called PP is a baseline configuration and allow tailored configurations to be layered on top. FedRAMP allows tailoring and overlays atop low, medium, high baseline requirements. Ample guidance for tailoring is obtained from NIST (National Institute of Standards and Technology, 2013). FedRAMP and ITSG-33 both encourage tailoring to baselines whereas CC is more restrictive as product must show at least demonstrable compliance to a PP

20. *Do requirements provide flexibility within security control requirements?*

    FedRAMP, CC and ITSG-33 allow assignment, selection, iteration and refinement operation. These actions support tailoring.

21. *Is there room to provide alternate requirements?*

    CC does not provide a way to provide alternate requirements. FedRAMP allows alternate requirements if assumptions about operational environment are not valid for a product. Such assumptions are also made by CC, but it is not clear about alternate route to take if product does not meet those assumptions. ITSG-33 allows requirements to be changes completely provided done in consultation with CCCS assessment team to verify if security objectives are still being met.

22. *Is the standard scalable?*

    CC allows delegation and automation that make certification scalable. FedRAMP while delegating and automating through 3PAOs also provides an alternate mode of authorization (JAB type) which has limited scalability due to less automation.

Transparency

23. *Does standard provide guidance on financial resources required for certification?*

    CC, FedRAMP, CCCS do not provide guidance on financial resources required for certification.

24. *Does standard communicate progress/time to completion?*

    CC, CCCS assessment framework, Assessment for FedRAMP through 3PAO do not indicate time to completion. This may be as assessment is delegated to third parties which may communicate progress during regular consultation sessions. FedRAMP process through JAB provides a rough timeline to complete each process.

Assessment Process Criteria

25. *Is evaluation delegated to third-party assessors(3PAO)?*

    Evaluation is delegated to third parties to provide CC and FedRAMP certifications. This is not the case to attest against criteria set by GC as CCCS personally evaluate for those standards.

26. *Is accreditation required for a 3PAO to operate as an assessment body?*

    CC requires 3PAOs to be certified with ISO/IEC 17025 in addition to fulfilling CCs own requirements. This is done to ensure that assessment is done fairly, consistently and reliably. FedRAMP also requires ISO/IEC 17025 certification along with additional requirements proposed in collaboration with A2LA. Assessment by CCCS does not mention any specific standards.

27. *Does standard provide criteria for evaluation of CSP?*

    CC provides clear criteria for evaluation in form on assurance requirements document. FedRAMP provides templates that must be used by 3PAOs during evaluation. However, criteria for evaluation is not clearly given. A SAP test case procedures template gives some idea about objectives of evaluations (FedRAMP, 2017). CCCS evaluated based on previous attestations and independent evaluations by CCCS members.

28. *Rate flexibility level given to third-party assessors to perform evaluation criteria or tests? Low, medium or high*

    CC and FedRAMP display medium level of flexibility as both provide criteria or requirements to test assurance. However, they allow 3PAOs to form test procedures to that fulfill assurance criteria. CCCS team allows high flexibility as assessment criteria is decided for each CSP on case-by-case basis.

29. *Is clear distinction provided between responsibilities of developer and authorizing body during assurance process? Yes*

    It is easy to find division of responsibilities in assurance documents of CC as they are provided with component description. With FedRAMP, division process is made clear by assigning templates to be filled by developer and assessors. The process of completing templates automatically delegates responsibility between developer and assessor. CCCS assessment framework does not provide clear distinction This is because certification process is unique to each CSP depending on previous attestations and risk analysis.

30. *Does assessment procedure explain limitations? Yes*

CC mentions assumptions that may turn into limitations in assessment process. FedRAMP does not mention limitations in its assessment framework. CCCS mentions limitations in its assessment process document. These are related to scalability, limited resources, and for product identified under high baseline category.

Reassessment and Continuous Monitoring

31. *Is reassessment mandatory? No*

CC does not ask for reassessment of security controls unless a major change is reported by developer. An impact analysis report (IAR) is submitted by developer to evaluator to track maintenance and in case of minor changes. FedRAMP calls this process continuous monitoring. However, FedRAMP evaluators assess security controls instead of asking developers to report changes. In case of major changes, either reported by developer using IAR by CC or assessed by evaluator during periodic maintenance in case of FedRAMP, re-evaluation process is initiated.

32. *Is continuous assessment frequency interval and related procedure decided between product developer and assessing body during evaluation phase of certification process?*

CC has formal procedure for assurance continuity where a fixed interval for reassessment is not decided beforehand. Reassessment is triggered if there are changes reported. Although not required by CC, a 3PAO may decide fixed interval in their evaluation scheme to increase reliability. Comparatively, FedRAMP asks that evaluators assess security controls at least annually. It also provides a template to help decide intervals in which to evaluate a control. CCCS assessment team decides a frequency interval on a case by case basis. This interval is decided after initial evaluation.

33. *Does standard require fixed frequency interval for reassessment?*
34. *If no, is frequency for reassessment flexible?*

Only FedRAMP mandates fixed interval for assessment for controls to be evaluated at least once annually. However, CC, FedRAMP and CCCS assessment offer option for frequency interval to be changes based on impact of changes to security of product.

35. *Are bodies conducting reassessment mentioned in standard documents?*

CC suggests that same evaluation bodies that offered original certification reassess as they will be with product. However, this is not stated as a requirement. Fair amount of trust is assumed between developer and evaluator as developers are responsible for notifying evaluators about changes. FedRAMP offers clear roles and responsibilities for various bodies such as FedRAMP PMO, JAB, AO, 3PAO in the reassessment process. CCCS performs reassessment for GC client. Further information about scope of their reassessment is lacking.

36. *Are procedures in place to address new vulnerabilities/changes?*

There are clear procedures in place in CC and FedRAMP standard. There is a separate process for vulnerabilities specifically under CC. In FedRAMP vulnerabilities for part of changes that may be found in product during periodic assessment. CCCS does not address vulnerabilities in their reassessment process. As mentioned, reassessment process is triggered due to request by GC client. The basis of this request in unclear.

37. *Are changes to product classified according to impact of change?*
38. *If yes, are each of these classifications described clearly in reassessment or standard documents?*

CC classifies changes according to impact to product and provides clear guidance on changes. FedRAMP also classifies based on impact of changes but does not provide clear guidance on classification. Information about this question is not mentioned in CCCS assessment documents.

39. *Is subset evaluation done in case changes are minor?*

CC and FedRAMP both allow subset evaluation of controls whose security if affected by said changes. The standards also assign responsibility of deciding controls to evaluating bodies. Information about this question is not mentioned in CCCS assessment documents.

40. *Do standard documents mention requirements that are not reassessed?*

In CC and FedRAMP, requirements that are not affected by changes to product are not reassessed.

41. *Does standard allow 3PAOs to be reassessed or monitored continuously?*

CC and FedRAMP allows reassessment of 3PAOs. They mention bodies that perform reassessment, but CC does not mention requirements for these reassessments.

Table 1: Results of Evaluation

Results of tested standards are provided in tabular form.

Security Profile Criteria	**CC**	**FedRAMP**	**ITSG-33**
1. Are documents/templates provided by standard that explain how to categorize into security profiles?	No	Yes	Yes
2. Does standard provide security profiles for cloud products/services specifically?	No	No	No
3. Does standard specify requirements to follow in case product belongs to multiple profiles?	Yes	Yes	Yes
4. Are CSPs pursuing authorization responsible for choosing their product's security profile? 5. If yes, does authorizing body validate the security profile? 6. Does authorizing body check security profile in early stages of authorization?	Yes Yes Yes	Yes Yes Yes	No Yes Yes
Privacy criteria			
7. Are privacy controls present?	Yes	Yes	No
8. Is conformance strict for all businesses and types of service providers?	No	No	No information available

9. Are privacy controls derived from legislation, policies, procedures, and/or associated controls?	Yes	Yes	No information available
Security Requirements Criteria			
10. Are requirements divided into suitable categories?	Yes	Yes	Yes
11. Is mapping of requirements between major standards available?	No	Yes	Yes
12. Do standards acknowledge dependencies in its requirements?	Yes	Yes	Yes
13. Do standards provide requirements or ways to obtain requirements for layered architecture such as IaaS, PaaS, SaaS?	No	Yes	No
14. Do requirements reference other documents, publications, templates that can provide more clarity on requirements?	Yes	Yes	Yes
15. Is physical infrastructure part of fulfilling requirements?	Yes	Yes	Yes
Flexibility			
16. Is this standard applicable in more than one country?	Yes	No	No
17. Is this standard a strict requirement for an industry/country?	No	Yes	Yes
18. Is this standard applicable in multiple industries?	Yes	No	No
19. Does standard provide baseline configurations and allow tailored configurations to be layered on top?	Yes	Yes	Yes
20. Do requirements provide flexibility within security control requirements?	Yes	Yes	Yes
21. Is there room to provide alternate requirements?	No	Yes	Yes
22. Is the standard scalable?	Yes	No	No
Transparency			
23. Does standard provide guidance on financial resources required for certification?	No	No	No
24. Does standard communicate progress/time to completion?	No	No	No

Assessment Process Criteria			
25. Is evaluation delegated to third-party assessors(3PAO)?	Yes	Yes	No
26. Is accreditation required for a 3PAO to operate as an assessment body?	Yes	Yes	No information available
27. Does standard provide criteria for evaluation?	Yes	No	No
28. Rate flexibility level given to third-party assessors to perform evaluation criteria or tests? Low, medium or high	Med	Med	High
29. Is clear distinction provided between responsibilities of developer and authorizing body about division of responsibility between developers and assessors?	Yes	Yes	No
30. Does assessment procedure explain limitations?	Yes	No	Yes
Reassessment and Continuous Monitoring			
31. Is reassessment mandatory?	No	Yes	No
32. Is continuous assessment frequency interval and related procedure decided between product developer and assessing body during evaluation phase of certification process?	No	Yes	Yes
33. Does standard require fixed frequency interval for reassessment? 34. Is frequency for reassessment flexible?	No Yes	Yes Yes	No Yes
35. Are bodies conducting reassessment mentioned in standard documents?	Yes	Yes	Yes
36. Are procedures in place to address new vulnerabilities/changes?	Yes	Yes	No information available
37. Are changes to product classified according to degree or impact of change? 38. If yes, are each of these classifications described clearly in reassessment or standard documents?	Yes Yes	Yes No	No information available
39. Is subset evaluation done in case changes are minor?	Yes	Yes	No information available
40. Do standard documents mention requirements that are not reassessed?	Yes	Yes	No
41. Does standard allow 3PAOs to be reassessed or monitored continuously?	Yes	Yes	No

F. Discussion of results

Section below describes conclusions of our comparative analysis methodology. Basis for comparison, scales used and general procedure for methodology are summarized in section 2 and available in detail in report #3 (Gupta, 2020). Results are derived after reference to report #3 and from evaluation and comparison between standards in section 3 and 4. To obtain more details about implications of results, report #3 can be seen. To obtain more information about tested standards, section D and E can be referred. The results of evaluation do not prove that one standard may be better than another, rather we use each criteria of evaluation to arrive at general conclusions about subject of criteria. We group multiple questions of a criteria to argue for a conclusion, if needed. Each question has been given a number is section D and E. We use the same scheme to refer to questions.

Security Profile Criteria

By answering question no. 1,3,4,5,6 affirmatively, we conclude that categorization process by FedRAMP and ITSG-33 is not straightforward and requires guidance from informative documents provided by standard. Selected profile is verified by assessors early in the evaluation process. This lowers chances of making mistakes by choosing the wrong security profile. We also conclude that by allowing CSPs to choose their own security profile, the standards save resources. This is because it is more efficient as CSPs understand their business goals to answer complex questions. For CC, we answer question no. 1 negatively. This makes the process of categorization more difficult which we conclude to be the case with CC. Based on answer for question 2, we conclude that security profiles of tested standards are not consistent with security objectives and risks of cloud services specifically.

These criteria can be used to evaluate other standards as well. However, a nuance that may affect conclusions from this criterion is that the basis for categorization into security profiles may be straightforward and hence guidance is not required. It may also be possible that categorization is very complex and thus standard offers consulting services to guide CSPs towards deciding relevant security profiles. To this end, deeper perusal into security profiles of a standard will be required.

Privacy criteria

Presence of privacy controls in an evaluation criterion for a standard. This criterion is fulfilled by FedRAMP and CC based on answer to question no. 7. Question no. 8 indicates that these controls are consistent and reliable. We conclude from question no. 9 that clarity has been provided about which businesses should conform to privacy controls for both these standards. ITSG-33 does not mention privacy controls so related questions are not applicable. We conclude that since ITSG-33 requirements are similar to FedRAMPs and NISTs that require privacy controls, CCCS assessment team for ITSG-33 will require privacy controls in some capacity. This evaluation criteria can be used for other standards as well.

Security Requirements Criteria

An affirmative answer for question no. 10,14 for CC, FedRAMP and ITSG-33 indicates that requirements are described in careful detail that allow easy implementation. We answer “no” to question no. 11 for CC. This means that if a product is certified with CC, it will be difficult to prove or transfer security controls to other standards. Answers to question no. 13 shows that all three standards reconcile security requirements between different dependencies. A negative answer for question 14 for CC and ITSG-33 indicates that dependencies for layered architecture is abstracted or expressed in general or related terms as is the case for CC. For ITSG-33, we conclude that consultation with standard bodies will be required to handle dependencies for IaaS, PaaS, SaaS. Question no. 15 provides informative knowledge about physical security. Evaluations for other standards can also be done using similar criteria.

Flexibility criteria

We answer “yes” to question no. 16,18,19,20 for CC. Hence CC is flexible and applicable to several industries in different countries. Acquiring knowledge of CC or being certified can be useful in understanding security requirements if a CSP that wants to offer services to a specific industry initially and diversify to include clients in other industries. FedRAMP and ITSG-33 are different in that they are only applicable to one type of industry, one country and are mandatory. Therefore, a CSP vendor that wishes to provide services to federal government of US or GC must be certified with FedRAMP and/or ITSG-33 requirements. However, security controls of all tested standards are flexible and allow parameters to be controlled by organization. From Question no 23, we see that CC is scalable. This means that CC allows delegation of responsibilities to multiple bodies that do not create a bottleneck. This is not the case for ITSG-33 and FedRAMP where authorization processes require services by few selected bodies which may get overwhelmed with increase in CSPs pursuing certifications. Evaluations for other standards can also be done using similar criteria.

Transparency criteria

Answering negatively to these questions can indicate lack of transparency by the standards. However, this can also indicate that task of providing guidance on financial resources and time to completion is delegated to assessing third parties or assessment bodies working closely with a CSP. This process works well for process designed to be carried out by third parties only but begs the question about transparency for procedures that require authorization or completion by the standard body. It is unclear if standards provide ways to communicate such information.

Assessment Process Criteria

We answer positively to question no. 26,27 for FedRAMP and CC to show assessment responsibilities are delegated to accountable parties by the standard. ITSG-33 assessment is conducted by CCCS and are not delegated to third parties. Answering yes to question no 28,30,31 for FedRAMP and CC shows clear description of criteria of evaluation is available with proper division of responsibilities and limitations of assessments are explained. Medium flexibility given to third-party assessors shows that 3PAOs make their own tests, but tests must fulfill expectations and objectives of evaluation criteria provided by standard body. High flexibility during CCCCS assessment shows that assessment committee form their own evaluation criteria with no evaluation criteria provided by standard body.

Reassessment and Continuous Monitoring

The higher the number of “yes” replies to questions posed about Reassessment and Continuous Monitoring, the more evidence is seen of a concrete, standardized process of reassessment that is well documented. By looking at answers for CC, we conclude that CC us flexible with reassessment process but provides a formal, documented procedure to provide a reliable reassessment process. FedRAMP also provides formal procedures for reassessment but requires mandatory reassessment. Effort has been made to cover new threats and save resources by providing subset evaluation for both FedRAMP and CC. CCCS reassessment procedures have not been documented. CCCS assessment team is delegated the process of reassessment. By not mentioning reassessment procedures, the standard has led us to believe that standardized reassessment procedures are not available but are decided on a case-by-case basis by CCCS

G. Conclusion

This report attempts to discuss important aspects of a cloud security standard by detailing features of CC, FedRAMP and ITSG-33. Similarities and differences between these standards are discussed, leading to conclusions being drawn about their repeatability, ease of certification, reliability by analyzing assessment and reassessment procedures. It is found that CC is a standard for IT security that states requirements at a high level of abstraction. In other words, it provides core principles that should be followed by other standards when defining requirements and assessment procedures so they can assure a secure product. FedRAMP draws heavily from NIST standard documents which are more technically specific in their requirements and assessment procedures. For example, privacy controls in CC following principles of unlinkability, anonymity, while NIST defines privacy controls in terms of data integrity, use limitation etc. CC and FedRAMP are comprehensive and procedures are defined for all scenarios. On the other hand, CCCS relies heavily on products that are certified with FedRAMP and ISO to establish credibility of a product. Thus, a product that is not certified with a standard recognized by CCCS, will face problems during implementation and assessment procedures. There are not clearly defined by the standard and are discussed on a case by case basis by CCCS using up their resources to do so. Future work will involve apply out evaluation criteria to other standards, comparing and drawing conclusions.

References

A2LA. (2019, December 12). *R311 - Specific Requirements: Federal Risk and Authorization Management Program (FedRAMP).* Retrieved from A2LA official website: https://a2la.qualtraxcloud.com/ShowDocument.aspx?ID=5621

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

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). *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. (2009, July). *Evaluation methodology.* Retrieved from https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R3.pdf

Common Criteria. (2012, June). *Assurance Continuity Requirements:CC.* Retrieved from https://www.commoncriteriaportal.org/files/operatingprocedures/2012-06-01.pdf

Common Criteria. (2014, July). *Arrangement on Recognition of CC ceritficates.* Retrieved from CC offical website: https://www.commoncriteriaportal.org/files/CCRA%20-%20July%202,%202014%20-%20Ratified%20September%208%202014.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. (2017, April). *Common Criteria Publications: Introductions and General Model.* Retrieved from Common Criteria official website: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5_marked_changes.pdf

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

Common Criteria. (n.d.). *Common Criteria: Categories of Protection Profiles*. Retrieved from Common Criteria official website: https://www.commoncriteriaportal.org/pps/

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

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

Common Criteria. (n.d.). *Members of CCRA*. Retrieved from CC official website: https://www.commoncriteriaportal.org/ccra/members/

Communication Security Establishment Canada. (2012, November). *IT Security Risk Management.* Retrieved from https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsg33-overview-apercu-eng_1.pdf

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

Cygnacom Certification Services. (2018). *Certifications: Cygnacom*. Retrieved from https://www.cygnacom.com/documents/CYG1005_CertServices_v7_1.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

EXECUTIVE OFFICE OF THE PRESIDENT,Office of Managment and Budget Washington. (2007). *Safeguarding Against and Responding to the Breach of Personally Identifiable Information.* Retrieved from White house offical website: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf

FedRAMP . (2011, December 8). *Cloud Service Providers: FedRAMP.* Retrieved from FedRAMP official website: https://www.fedramp.gov/assets/resources/documents/FedRAMP_Policy_Memo.pdf

FedRAMP. (2017, December). *FEDRAMP 3PAO OBLIGATIONS AND PERFORMANCE GUIDE.* Retrieved from FedRAMP official wesbite: https://www.fedramp.gov/assets/resources/documents/3PAO_Obligations_and_Performance_Guide.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, June). *Privacy Impact Assessment Template: FedRAMP.* Retrieved from https://www.fedramp.gov/assets/resources/templates/SSP-A04-FedRAMP-PIA-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). *Security Assessment Framework: FedRAMP.* Retrieved from https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Assessment_Framework.pdf

FedRAMP. (2018, April). *FedRAMP Continuous Monitoring Strategy Guide.* Retrieved from Fedramp offical website: https://www.fedramp.gov/assets/resources/documents/CSP_Continuous_Monitoring_Strategy_Guide.pdf

FedRAMP. (2018, August). *FedRAMP Laws and Regulations Template.* Retrieved from https://www.fedramp.gov/assets/resources/templates/SSP-A12-FedRAMP-Laws-and-Regulations-Template.xlsx

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). *FedRAMP Significant Change Request Form.* Retrieved from FedRAMP official website: https://www.fedramp.gov/assets/resources/templates/FedRAMP-Significant-Change-Form-Template.pdf

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. (n.d.). *Agency Authorization Process: FedRAMP*. Retrieved from FedRAMP offical website: https://www.fedramp.gov/agency-authorization/

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

FedRAMP Fast Forward Industry Advocacy Group. (2016, January). *Fix FedRAMP Press Release.* Retrieved from https://www.meritalk.com/wp-content/uploads/2016/01/Fix-FedRAMP-Press-Release_FINAL.pdf

FedRAMP. (n.d.). *Get Authorized: Joint Authorization Board*. Retrieved from https://www.fedramp.gov/jab-authorization/

FedRAMP. (n.d.). *Third Party Assessment Organizations: FedRAMP*. Retrieved from https://www.fedramp.gov/assessors/

Gupta, V. (2020). *Comparative Analysis Methodology.* Ottawa.

Gupta, V. (2020). *Literature Survey: Cloud Security Evaluation Approaches.* Ottawa.

International Organization for Standardization. (1947). *About us: International Organization for Standardization*. Retrieved from https://www.iso.org/about-us.html

Intertek EWA Canada. (n.d.). *Common Criteria Evaluations*. Retrieved from Intertek Official Website: https://www.intertek.com/cybersecurity/testing/common-criteria/

ISACA. (2019). *COBIT 2019 Publications & Resources*. Retrieved from ISACA corportation website: http://www.isaca.org/COBIT/Pages/COBIT-2019-Publications-Resources.aspx

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