Methodology for Comparing Cloud Computing Security Standards

By Vidushi Gupta

Introduction

Previous reports described security control requirements of cloud computing security standards and evaluation processes undertaken by standards to assess whether a cloud service providers (CSP) is certifiable with the standard's certificate. Specifically, previous work focused on the FedRAMP standard, TBS Cloud Security Profile and ISO 15408 (common criteria). Their assessment processes were discussed alongside points of comparison between these evaluation methods. As number of CSPs increase with the goal of capturing a large share of market by providing cloud services to different industries, requirement to be complaint with different standards also increases. Hence, criteria of classifying different standards based on requirements, evaluation and compatibility with different industries is required. Therefore, this report attempts to introduce a methodology to evaluate cloud security standards. Once CSPs are aware of their business objectives and their product, they can use this criterion to compare between different standards. This methodology is limited in the sense that it does not attempt to reconcile business goals of a CSP with best standard that fits it. Instead it attempts to compare different standards based on features that are found within a standard.

Methodology

The proposed methodology attempts to evaluate cloud security standards based on 7 criteria based on security profiles, security requirements, privacy controls, flexibility, transparency, assessment process, reassessment and continuous monitoring. A report is presented on aspects of cloud security standard that can be used to distinguish or evaluate it compared to other standards. The criteria are derived based on common standards such as NIST.SP.800.53 (NIST, 2015), FedRAMP (FedRAMP, n.d.), ITSG-33 (Communication Security Establishment Canada, 2012) and ISO 15408 or common criteria (Common Criteria Recognition Arrangement).

NIST and common criteria provide standards for IT products in general. They are tailored for cloud services and certified through FedRAMP. ITSG is also derived from NIST and FedRAMP. By using standards applicable to cloud products and information systems in general, there was an attempt to obtain big picture elements of security standards so this methodology can be repeatable. Main points of differences were found between these standards and critical analysis was done to ask questions that distinguish one standard from another. An appendix is provided with a summary of analysis in form of yes/no questions. Answers to these questions highlight key differences that are useful in understanding a standard comprehensively, which may further influence decisions in choosing which standards to comply with. These criteria are limited in that, finer points of

comparison are not included. For example, comparison between specifics of functional requirements or assessment tests to evaluate differences has not been done. Usage of words such as product developers and developers refer to organization personnel involved in pursuing authorization. Standard body is used interchangeably with authorizing body and refers to the certifying organization.

Evaluation Criteria for Comparing Standards

Security Profiles Criteria

According to (NIST, 2004), "categorizing information and information systems into security profiles provides a common framework and understanding for expressing security that promotes effective management of information security systems across communities, consistent reporting to managing authorities on competence of information security policies, procedures and practices". It categorizes information systems into security profiles for use in federal government, the process of categorization can be found consistent among cloud security standards applicable to other industries. Standards may categorize information systems into type of products (e.g. firewalls, access management systems) and offer security requirements depending on type of IT product. A standard may also categorize requirements based on impact to mission, assets, day-to-day functions, individuals in case of security breach to an information system. This type of classification is called impact analysis classification (NIST, 2015).We will evaluate a standard based on if it allows classification of IT products and services including cloud services into categories or security profiles. We will describe the basis for this categorization - if it is done on impact analysis, type of product or another. This evaluation is important as it eases the process of categorization, the first step for a CSP that is pursuing certification to a standard. To allow easy and consistent classification, it is also important that guidance is provided by a standard on how to categorize a system into these categories. Providing examples of type of service along with its classification is helpful.

Additionally, we will also mention if the process of categorization is standardized. This further ensures that categorization process is reliable, consistent and repeatable. This will also ensure that additional resources are available to pursuant developers for guidance, if needed. We will mention if a standard is specifically meant for cloud security or security of any type of information system. If a standard caters to cloud services, security profiles are specific consistent with security objectives of a CSP. However, it is also possible that security profile remains the same irrespective of whether the standard caters to CSPs specifically or any information system in general.

For categorization based on type of product, each type has its own security requirements. Here, unlike classification using impact analysis which may be hierarchical, meaning business activities judged to have high impact must adhere to low and moderate security profile baseline in addition

to high quality baseline, classification based on type of product is expected to have less overlap in security requirements between different products. As an example, products claiming conformance to security profile for Firewalls need to implement requirements for security attribute-based access control while those conforming to security profile for an Enterprise Security Management Access Control product do not. This distinction is of importance when one product may belong to two security profiles simultaneously especially where one component or function of a product is distinct enough to belong to another security profile compared to main product. In that case, a standard must provide guidance on which security profile a product must comply with. Similarly, with impact-level type of classification, some components or function of a system may have impacts on multiple levels meaning security breaches on one component of the system might have low impact while another has high impact. Which security profile's security requirement should a CSP conform to if it has multiple impact levels? If a product belongs to multiple product types, should it fulfill requirements from all product types?

Another criterion for evaluating a standard is whether it requires a CSP pursuing authorization to independently categorize their product into a security profile. This is the case for standards that provide ample resources in form of documents and templates to help CSPs make the right choice for a security profile. The CSP may have the option to hire third-party consulting bodies to help. Allowing CSPs to choose their own security profile is efficient as CSPs understand their business goals to answer complex questions that decide a product's security profile. It also allows the standardizing body to save resources. However, the responsibility of verifying if correct profile is chosen falls on bodies assessing a standard. If CSP makes a mistake in choosing their security profile and consequently have not implemented appropriate requirements, this can lead to wastage of time and money. Assessing a chosen security profile with standardizing body would be beneficial. Assessing a standard based on who is responsible for choosing security standard and then verifying the choice is our next criteria. This criterion raises a larger question about how involved the authorizing body is in the process of authorization during assessment and reassessment.

Privacy criteria

Security concerns are intertwined with privacy concerns. In 1974, the privacy act sought to maintain balance between individual's information needed by organizations with individuals right to be kept aware of how that information was collected, maintained and disposed of after period of use. With the proliferation of cloud computing, along with social media, mobile computing, there is greater challenge in controlling confidentiality and integrity of a person's information (NIST, 2015).

Presence of privacy controls in an evaluation criterion for a standard. If these privacy controls are derived from legislation, policies, procedures, and associated controls, their consistency and reliability increases. OMB memorandum 07-16 defines Personally Identifiable Information (PII), as some unit of information about an individual that can be traced back to the person's identity

(NIST, 2015). Therefore, privacy controls seek to ensure proper handling of PII. Most CSPs collect personal user information and hence will be required to adhere to privacy controls. However, depending on if standards are applicable to CSPs or all IT products and if they collect, process or store PII, a standard may leave privacy controls optional. Therefore, standards must have formal procedures to let a business decide if it is required to enforce privacy controls based on criteria. Whether strict conformance is necessary and if no, clarity about which type of businesses are required to adhere to privacy controls will be part of our evaluation criteria.

If privacy controls are required to be implemented, questions can be asked about if they are evaluated by authorizing bodies during assessment process. If yes, are they also part of reassessment process? Are privacy controls structured like security controls where they are arranged according to families and security profiles? Knowledge about extent of privacy requirements by a standard gives insight into privacy concerns and potential threats about privacy breaches.

Security Requirements Criteria

Like security profiles, it is important that security requirements are presented in an understandable and categorical way to make it easy for CSPs to understand and implement them. Standards may divide their requirements into categories (e.g. technical, operational or management controls) to make it easy for developers to decipher requirements. Some standards may not contain all classes of requirements and thus are required to refer to a standard that contains that category of requirements. A notable example of category of requirement missing in Fedramp are those related to cryptography.

In cases where compliance with two different standards is required and to make it easy to compare between requirements, it is important that a mapping between control categories is provided. Also, many information technology architectures including cloud technologies exhibit dependencies to other products and technologies. Providing a way to reconcile security requirements between different dependencies is essential for a standard. This may involve having a separate class that states requirements on how to report dependencies and delegate responsibilities of implementing security requirements to appropriate parties developing this inter-dependent layered architecture. Dependency requirements may also ask for isolating functions to have less interdependencies to make them more manageable and secure.

Flexibility Criteria

To save time and money, a standard should be applicable to several industries and different countries. This is especially important for a CSP that wants to offer services to a specific industry initially and diversify to include clients in other industries. For example, Microsoft wants to offer its email software to government workers in Canada, United Nations and to universities in different countries around the world.

It makes sense that a standard that is more flexible will not cater to a specific type of information services with requirements about specific technologies. Instead, a flexible standard will allow product developers to tailor requirements while also maintaining reliability. If we focus on security requirements of standards, both for standards pertaining specifically to cloud computing or to IT products in general, some flexibility is required during implementation of requirements. This leads to baseline requirements i.e. requirements under a security profile that must be implemented strictly. However, if assigned parties, either developer of product or assessing parties, find the need for more security controls, they can be implemented. Thus, there needs to be acknowledgement that one set of requirements will not meet all security needs of various architectures.

Another type of criteria for flexibility is to allow some features of a requirement to be decided by the organization pursuing compliance. For example, there may be a requirement to develop, document and disseminate system and communication protection policy and procedures that must be followed strictly. However, organization personnel or roles who are on receiving end of this information may be decided by the organization. If an organization is not able to implement a requirement, there should be room to suggest an alternate requirement. Formal procedure to do so may not be available in a standard as such a tailored requirement cannot be generalized for different products.

Our final criterion is to ask if a standard is scalable? This means that if large quantities of CSPs enter the market, is the standard able to provide certifications at a steady pace? Historical evidence about a standard can be investigated to gain insight into this criterion.

Transparency Criteria

Due to volume of requirements to be implemented followed by series of assessments to ensure implementation, pursuing certification involves a series of stages with developers of products and certifying bodies. It is important to keep CSPs informed about progress regularly so CSPs can allocate resources accordingly. Such transparency can be in form of regular contact between authorizing body or can be automated. Information can also be relayed between CSPs and authorizing body about approximate time it will take to complete authorization. Cost of authorization can also be communicated. Our criterion is to evaluate if a standard has such processes that promote transparency.

Assessment Process Criteria

Once a CSP implements security controls relevant to security profiles, these controls are then evaluated by certifying authorities. The process of evaluation or assurance is done by officials from a standard body or is delegated to third-party assessment organization(3PAO).The distinction between who is evaluating is an important criterion for our assessment of a standard. If standard body is directly authorizing and performing assessments, there is an advantage of transparency as the CSP obtains feedback of assessment directly from officials of standardizing

bodies. On the other hand, standard may not have resources to assess directly and may delegate the process to 3PAO. This may decrease transparency. There might also be different weights provided to evaluation done directly by standard officials versus those done by 3PAO, whether stated explicitly by standard body or not.

If third-party assessors are providing assurance on behalf of the standard, questions arise about how they are chosen as authorizing party. This aspect will form one of our criteria about evaluations. Also, most standards provide a criterion for assessing if security requirements are implemented by CSP. Some standards may provide very specific criteria with tests and procedures to be performed and templates with fixed format on results to be recorded. Other standards might provide evaluation criteria but allow authorized 3PAOs to design their own tests for evaluation provided these tests fulfill the criteria provided by standard body. Based on criterion of flexibility provided to 3PAO to perform evaluations, we define a scale with three levels of flexibility: low, medium, high.

High flexibility: 3PAOs form their own evaluation criteria with no evaluation criteria provided by standard body.

Medium flexibility: 3PAOs make their own tests but tests must fulfill expectations and objectives of evaluation criteria provided by standard body.

Low flexibility: Standard body provides specific tests (for some or all requirements), templates and documents that must be used to report results of evaluation.

Medium level of flexibility is necessary for a standard that is catering to large number of industries in different countries and does not have resources or expertise to directly evaluate an information system. While those providing low flexibility can automate the assessment process by ensuring uniformity and consistency. During assessment process, the responsibilities of developers and assessors must be made clear by the assessors. For example, assessors might require developers of product to conduct some tests and report results to assessors before evaluation can begin. Lastly, we evaluate standards based on if they convey limitations of their assessment process. As an example, standards may not evaluate physical infrastructure or privacy controls during assessment.

Reassessment or Continuous Monitoring Criteria

We begin by evaluating if a standard has formal procedures for continuous monitoring of a certified product to ensure that security controls are implemented without disruption and compromise. A standard should clarify if all or a subset of requirements need to be reevaluated. Some standards may provide a fixed time period after which reassessment is invoked or may allow frequency to be tailored to product during assessment process. Additionally, some standards may reassess if changes occur to a product that affect its security capabilities. In that case, a standard may have procedures to evaluate the degree to which security is affected and

requirements that need to re-evaluate. This process is tailored as each product undergoes different changes to its features and function. Guidance may be provided by the standard to ensure that all parameters of a change have been considered. It may also be required for a developer to report changes in a specific manner. A standard might ask for periodic reports to be sent to authorizing body irrespective of change to a product. On the other hand, reports are required only in case there is change and a reassessment is required. Within change to a product as a criterion, change can be classified as small, medium or large as defined by the standard. For example, are changes to hardware classified as a change? Changes to development environment? Changes to threat assumptions, security objectives? A CSP may only be asked to report some changes that lead to reevaluation. Hence, only a subset of changes will cause a reassessment. These decisions prepare CSPs with procedures in order to stay certified with standard. Furthermore, are there any requirements that are not addressed as part of reassessment? For example, reassessment procedures to evaluate privacy requirements may not exist. Lastly, since 3PAOs play a significant role in certification and reassessment process, it is important that their processes are accountable and current. We will discuss and evaluate if a standard allows 3PAO to be reassessed.

Conclusion

Security standards for cloud products are heavily influenced by requirements to ensure security for IT products. The criteria presented in above report describe subjects of key differences between standards. Evaluating a standard based of these criteria will provide a comprehensive picture about a standard's processes and procedures. Future work will involve evaluating some common standards (NIST, Fedramp, Common Criteria) against these criteria and deriving appropriate conclusions.

Appendix

Security Profile Criteria	
Are documents/templates provided by standard that explain how to categorize into security profiles?	Yes/no
Does standard provide security profiles for cloud products/services specifically?	Yes/no
Does standard specify requirements to follow in case product belongs to multiple profiles?	Yes/no

Are CSPs pursuing authorization responsible for choosing their product's security profile? If yes, does authorizing body validate the security profile? Does authorizing body check security profile in early stages of authorization?	Yes/no
Privacy criteria	
Are privacy controls present?	Yes/no
Is conformance strict for all businesses and types of service providers?	Yes/no
Are privacy controls derived from legislation, policies, procedures, and/or associated controls?	Yes/no
Security Requirements Criteria	
Are requirements divided into suitable categories?	Yes/no
Is mapping of requirements between major standards available?	Yes/no
Do standards acknowledge dependencies in its requirements?	Yes/no
Do standards provide requirements or ways to obtain requirements for layered architecture such as IaaS, PaaS, SaaS?	Yes/no
Do requirements reference other documents, publications, templates that can provide more clarity on requirements?	Yes/no
Is physical infrastructure part of fulfilling requirements?	Yes/no
Flexibility	
Is this standard applicable in more than one country?	Yes/no
Is this standard a strict requirement for an industry/country?	Yes/no
Is this standard applicable in multiple industries?	Yes/no
Is compliance to this standard transferrable to different industries and/or countries?	Yes/no
Does standard provide baseline configurations and allow tailored configurations to be layered on top?	Yes/no
Do requirements provide flexibility within security control requirements?	Yes/no
Is there room to provide alternate requirements?	Yes/no

Is the standard scalable?	Yes/no
Transparency	
Does standard provide guidance on financial resources required for certification?	Yes/no
Does standard communicate progress/time to completion?	Yes/no
Assessment Process Criteria	
Is evaluation delegated to third-party assessors(3PAO)?	Yes/no
Is accreditation required for a 3PAO to operate as an assessment body?	Yes/no
Does standard provide criteria for evaluation?	Yes/no
Rate flexibility level given to third-party assessors to perform evaluation criteria or tests? Low, medium or high	Low/Med/High
Is clear distinction provided between responsibilities of developer and authorizing body about division of responsibility between developers and assessors?	Yes/no
Does assessment procedure explain limitations?	Yes/no
Reassessment and Continuous Monitoring	
Is reassessment mandatory?	Yes/No
Is continuous assessment frequency interval and related procedure decided between product developer and assessing body during evaluation phase of certification process?	Yes/no
Does standard require fixed frequency interval for reassessment? If no, is frequency for reassessment flexible?	Yes/no
Are bodies conducting reassessment mentioned in standard documents?	Yes/no
Are procedures in place to address new vulnerabilities/changes?	Yes/no
Are changes to product classified according to degree or impact of change? If yes, are each of these classifications described clearly in reassessment or standard documents?	Yes/no
Is subset evaluation done in case changes are minor?	Yes/no

Do standard documents mention requirements that are not reassessed?	Yes/no
Does standard allow 3PAOs to be reassessed or monitored continuously?	Yes/no

References

Common Criteria Recognition Arrangement. (n.d.). *home: common criteria website.* Retrieved from https://www.commoncriteriaportal.org/

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

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

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

NIST. (2015, january). *Security and Privacy Controls for Federal Information Systems and Organisations: NIST 800-53.* Retrieved from NIST official website: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf