LAUREA
UNIVERSITY OF APPLIED SCIENCES
Together we are stronger

Cloud Security Audit for A Certification and Training Center

Otieno, Duncan

Laurea University of Applied Sciences
Leppävaara

Cloud security audit for a certification and training center

Otieno Duncan
Degree Programme in BIT
Bachelor's Thesis
March, 2018

Laurea University of Applied Sciences **Abstract**
Degree Programme in Business Information Technology
Bachelor's Thesis

Otieno, Duncan

Cloud security audit for a certification and training center

Year 2018 Pages 67

This thesis project was commissioned by Data To Information College. This is a technical education, training and certification center for both local and international examinations. The institution is located in Eldoret, Kenya. The thesis audits the organization in five control domains for compliancy. A Continous Assessments Initiative Questionnaire (CAIQ) by the Cloud Security Alliance is used for the security audit.

In the empirical section, an audit finding was carried out to determine the state of the organization's security while accessing and using the cloud. The audit was carried out for the following domains: Audit Assurance & Compliance, Business Continuity Management & Operational Resilience, Governance and Risk Management, Security Incident Management, Threat Vulnerability Management. A business impact analysis (BIA) was carried out on 18 sub-controls that were not compliant. Qualitative and semi-quantitative analysis were used to determine the level of criticality and risk levels respectively.

A total of 41 questions were asked during the audit and 18 sub-controls were compliant, 18 were non-compliant and 5 were marked as 'N/A' which were either confidential or the auditee didn't know the answer. Out of the sub-controls that were non-compliant, 11 posed a high risk level for the organization, 4 - medium risk level and 3 – low risk level.

In conclusion, the researcher recommended that the organization undertake a threat vulnerability management program to address the non-compliant sub-controls that had a high risk level to operational impact of the organization. A list of safeguards to be implemented against known threats was also presented.

Keywords: cloud computing, threat, malware, cloud compliance, security, CSA

Table of contents

Keywords

Cloud computing “is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models” (NIST 2009).

Threat “A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm” (RFC 2828).

Malware “is a software that has some harmful purpose, by itself or as a part of a bigger system” (Gregory 2015, 41).

Cloud compliance “is an assurance that the cloud-delivered systems must be following the standards that the cloud customers face” (Techopedia 2018).

Security “The condition of a system that results from the establishment and maintenance of measures to protect the system” (RFC 2828).

CSA (Cloud Security Alliance) “is the world’s leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment.”

1 Introduction

This research-based thesis aims at investigating the threats Data to Information College faces in their day-to-day use of cloud services. This is accomplished by carrying out an I.T. audit and following the guidelines outlined in the Cloud Security Alliance (CSA) Framework to determine the type of threat and risk level. The overall results of the thesis will enable the client company to be able to take outlined measures in order to protect their data and privacy in the cloud.

The author begins the chapter by introducing the background information for the thesis, aims and objectives, research problem, keywords, and case company.

1.1 Background

Cloud computing technology has revolutionized the way data is stored, accessed and transferred. It is now possible to store and access huge amounts of data off-the-premise without the need or worry of physical storage space. In addition to the regular threats to network security, the unique nature of cloud computing creates a different type of threats that are available only in a cloud environment (Alani 2014, 2).

In their The Treacherous Twelve, Cloud Security Alliance have identified twelve threats that represent most important threats to cloud computing in the year 2016. “The threats identified serves as an up-to-date guide that will help cloud users and providers make informed decisions about risk mitigation within a cloud strategy” (Cloud Security Alliance 2016).

The case company for this thesis, Data To Information College, is a certification center that handles confidential students’ data which is vital for protection and privacy since they store their data in the cloud. Security breaches could jeopardize the running of the organization and confidence from the students. “The CIA (Confidentiality, Integrity, and Availability) triad of information security is an information security benchmark model used to evaluate the information security of an organization. The CIA triad of information security implements security using three key areas related to information systems including confidentiality, integrity and availability” (Techopedia 2018).

Data To Information College started using cloud computing technology in the year 2016. This has greatly benefitted the company in-terms of cost-saving and resource personnel, however it is facing information security challenges while using the technology. This created a need for research to be conducted in to find out loopholes in the organization’s information security structure.

1.2 Thesis objective

The thesis aims at analyzing the current situation in the organization by carrying out an IT audit and then proposing a list of controls to be implemented based on the CSA framework.

The objectives of this project are:

- Determine the current state of cloud security by carrying out an audit based on Consensus Assessments Initiative Questionnaire.
- Document the current state of the cloud computing service model
- Perform a business impact analysis (BIA) to determine risk level and recovery plan
- Publish a list of controls to be implemented based on Cloud Security Alliance security guidance.

1.3 Case company

The case company for the thesis is Data To Information College. It is a privately owned institution that was started in the year 2002 as a technical education, Training and Testing Center for both local and foreign exams (d2ikenya 2014).

The college is only one of the three certified test centers for Test Of English as a Foreign Language (TOEFL) in the country, with the rest two located in the capital city of Kenya. It is affiliated with several major companies in the I.T industry such as Microsoft, Pearson VUE, CompTIA, SAT, IELTS and CISCO By the end of year 2017, the college had 20 staffs and average of 150 students (d2ikenya 2014).

2 Threat Mitigation in Cloud Computing

This chapter studies various theories from books, journals and internet sources regarding cloud computing. The outcome will be secondary data in regard to the thesis outcome. This chapter aims to illustrate the inception of cloud computing and threats faced.

2.1 Defining cloud computing

Many cloud experts and vendors have tried to define what cloud computing is. According to (Chandrasekaran 2015, 12) “cloud computing is a means of storing and accessing data and programs over the Internet from a remote location or computer instead of our computer’s hard drive. This is one of the simplest terms and it is only provides a representative of the whole definition.”

NIST 800-145 puts forth a formal definition of cloud computing as a “model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” (Mell & Grance 2011).

The definition from NIST gets a backing from International Standards Organization (ISO), Cloud Security Alliance (CSA) and the Institute of Electrical and Electronics Engineers (IEEE). This is why it is more agreed by vendors, experts and pundits.

National Institute of Standards and Technology (NIST) went further ahead by putting forth a 5-4-3 principle that describes “(a) the five essential characteristic features that promote cloud computing, (b) the four deployment models that are used to narrate the cloud computing opportunities for customers while looking at architectural models, and (c) the three important and basic service offering models of cloud computing” (Chandrasekaran 2015, 14.)

Cloud computing model has been visualized by Mogull, Arlen, Gilbert, Lane, Mortman, Peterson and Rothman (2017, 11) in their book security guidance as shown in Figure 1.

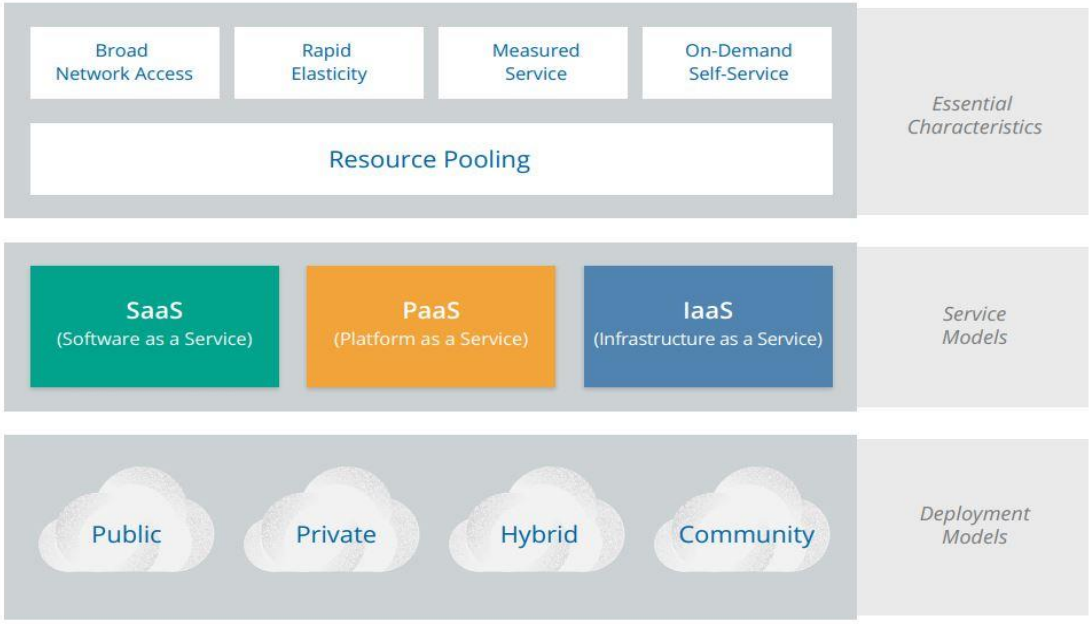


Figure 1: Visualization of cloud computing (Mogull et al. 2017, 10)

2.1.1 Essential characteristics

There are five essential characteristics that define a cloud as implied by NIST.

The table below summarizes these characteristics.

Element	NIST description
Resource pooling	It is the most fundamental characteristic. The provider abstracts resources and collects them into a pool, portions of which can be allocated to different consumers (typically based on policies).
On-demand self-service	A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
Broad network access	It means that all resources are available over a network, without any need for direct physical access; the network is not necessarily part of the service.
Rapid elasticity	This allows consumers to expand or contract the resources they use from the pool (provisioning and deprovisioning), often completely automatically. It also allows them to more closely match resource consumption with demand (for example, adding virtual servers as demand increases, then shutting them down when demand drops).
Measured service	Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

Table 1: Essential characteristics of cloud computing (Mogull et al. 2017, 10)

These essential characteristics means that cloud computing enables businesses and companies to be able to operate freely and cheaply without the need for large personnel teams, expensive hardware, software and networking resources.

2.1.2 Service models

Cloud service offering models are divided into three classes, namely: (1) Software as a Service, (2) Platform as a Service, and (3) Infrastructure as a Service. Additionally, there is also the hardware layer and abstraction layer of software. The hardware layer contains processors, memory and storage components while the abstraction layer of software which lies below Infrastructure as a Service (IaaS) acts as a hypervisor by realizing the unique characteristics of cloud computing.

In his book on securing the cloud, Alani (2014, 2) outlines the various layers of cloud computing as shown in Figure 2.

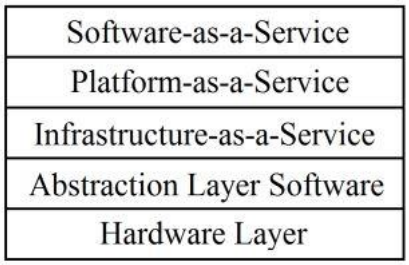


Figure 2: Layers of cloud computing (Alani 2014, 2)

Software as a Service (SaaS):

This is a full application that resides on top of the cloud stack. It's managed and hosted by the provider and the applications can be accessed via thin client interfaces such as a web browser or a program interface.

Platform as a Service (Paas):

"This layer gives the capability to deploy consumer-created or acquired applications using programming languages and tools supported by the provider" (Marinescu 2013, 32).

According to Mogull et al. (2017, 11) Application Programming Interfaces (API) access to features of a full SaaS application. The key differentiator is that, with PaaS, you don't manage the underlying servers, networks, or other infrastructure.

The figure below shows Paas running on top of IaaS architecture according to Cloud Security Alliance.

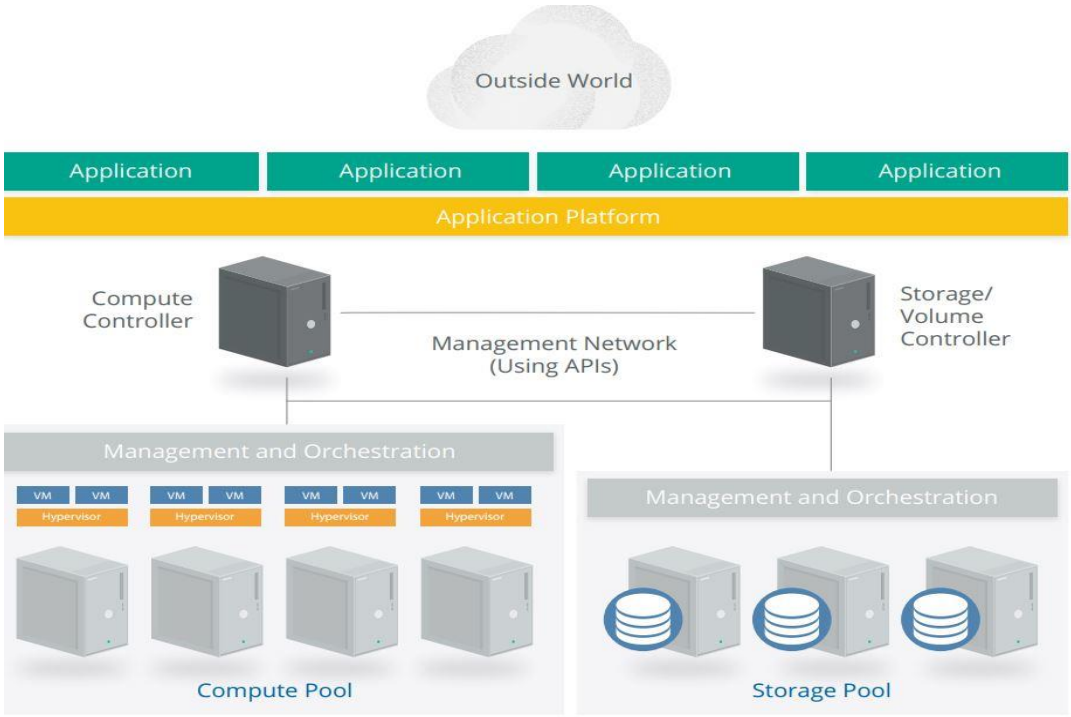


Figure 3: PaaS running on top of IaaS architecture (Mogull et al. 2017, 17)

Infrastructure as a Service (IaaS):

This is the lowest service level provided to the client. IaaS provides the cloud computing client with controlled access to the virtual infrastructure whereby the client can install operating system and application software. In this model, the client manages the security aspects from the operating system up to the application software but doesn't control the physical hardware.
Iaas offers a huge responsibility in terms of security and thus is not popular among clients. In Iaas, the clients runs most of the management duties while in Paas the vendor manages everything.

Figure 4 below shows Iaas architecture.

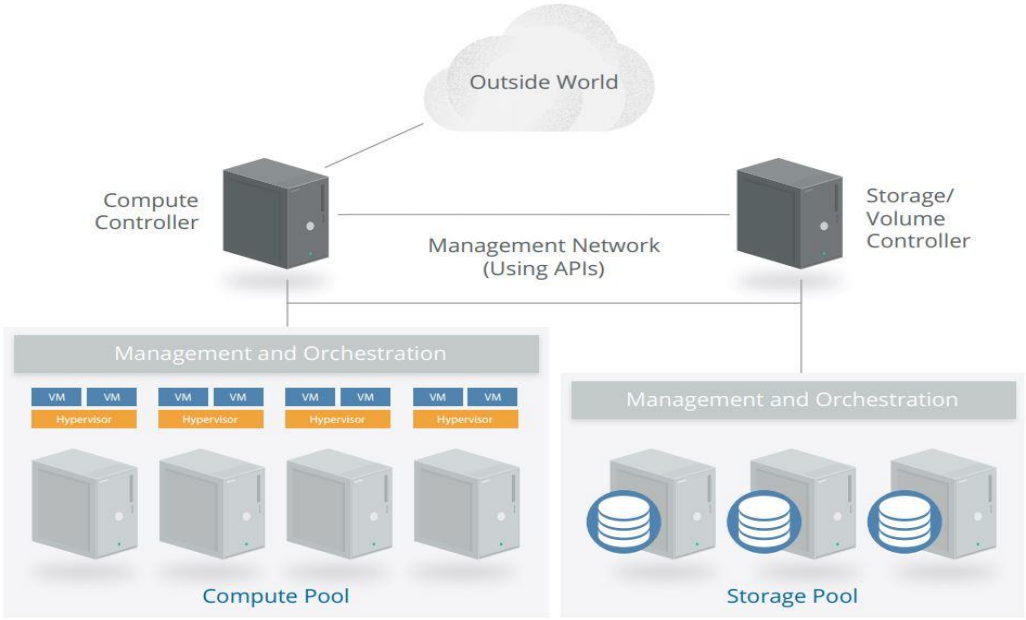


Figure 4: Compute IaaS platform architecture (Mogull et al. 2017, 11)

2.1.3 Deployment models

According to Mogull et al. (2017, 11), both NIST and ISO/IEC use four cloud deployment models.

Public cloud:

The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Private cloud:

The cloud infrastructure is operated solely for a single organization. It may be managed by the organization or by a third party and may be located on-premises or off-premises.

Community cloud:

The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns. It may be managed by the organizations or by a third party and may be located on-premises or off-premises.

Hybrid cloud:

The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

2.2 Cloud ecosystem

According to Chandrasekaran (2015, 41) cloud ecosystem is a term used to describe the complete environment or system of interdependent components or entities that work together to enable and support the cloud services. This ecosystem contains complex entities that interacts with other components and organization with individuals (actors) who are responsible for providing and consuming cloud services.

There are three actors in a cloud ecosystem:

a) Cloud Service Users (CSU),
b) Cloud Service Providers (CSP),
c) Cloud Service Partners (CSN).

Figure 5 illustrates how the three actors are involved in a cloud ecosystem.

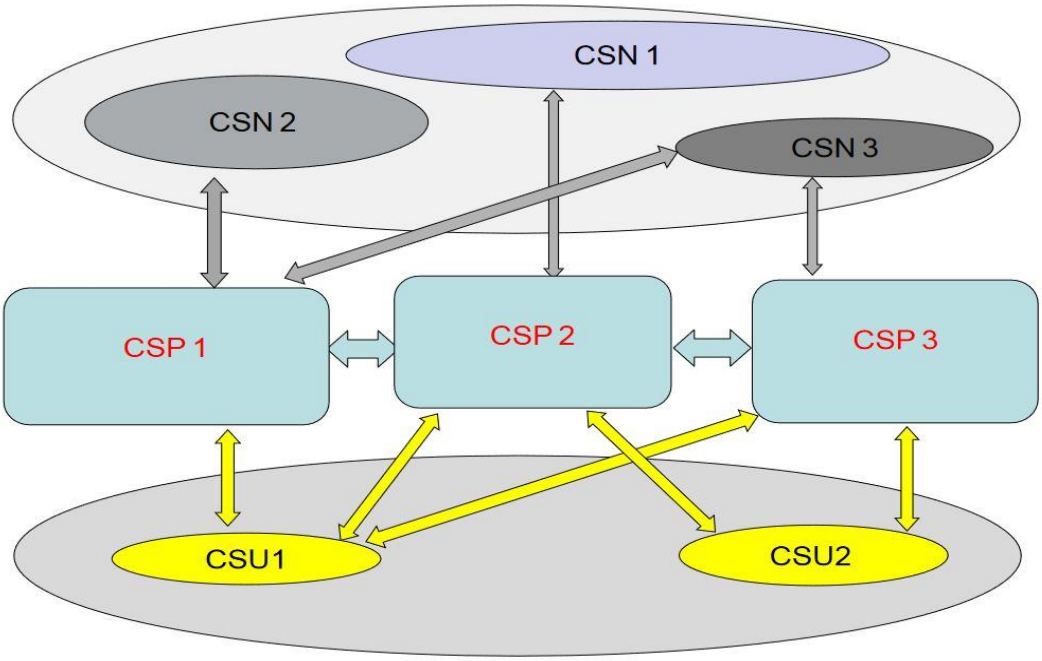


Figure 5: The three actors of a cloud ecosystem (ITU 2012, 13)

Cloud Service Users (CSU)

This is a consumer, organization or enterprise that makes use of the delivered cloud services. An intermediate user that delivers the cloud services to the end user can also be a CSU. These end users may include applications, persons or machines (Chandrasekaran 2015, 42).

Cloud Service Providers (CSP)

“An organization that provides or delivers and maintains or manages cloud services, that is, provider of SaaS, PaaS, IaaS, or any allied computing infrastructure” (Chandrasekaran 2015, 42).

Cloud Service Partners (CSN)

“A person or organization (e.g., application developer; content, software, hardware, and/or equipment provider; system integrator; and/or auditor) that provides support to the building of a service offered by a CSP (e.g., service integration)” (Chandrasekaran 2015, 42).

The figure below shows how actors interact in a cloud ecosystem.

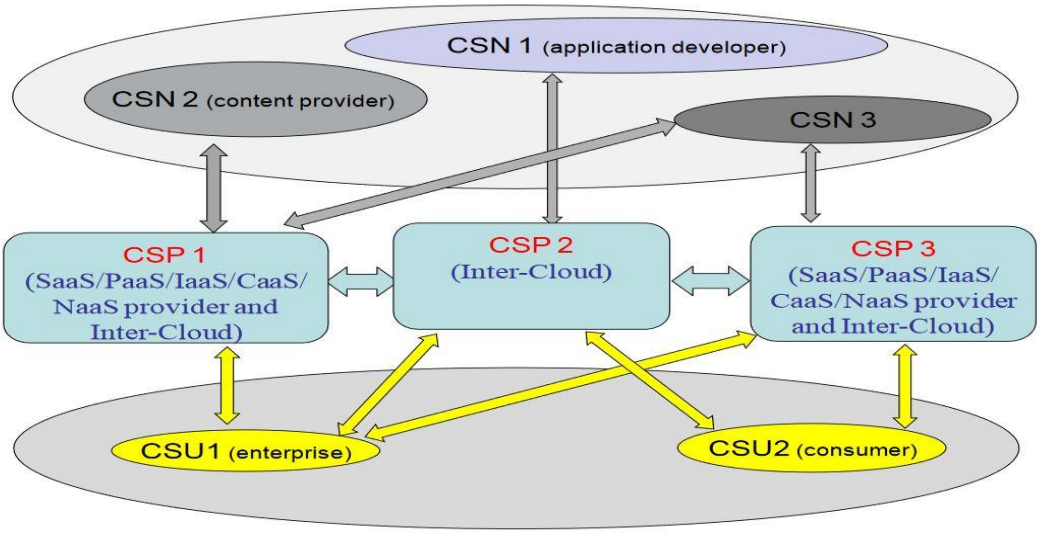


Figure 6: Actors with some of their possible roles in a cloud ecosystem (ITU 2012, 13)

From the concepts illustrated in subchapters 2.1.3 and 2.2, cloud service models require certain features to be exhibited in order to be considered as services. The following are basic requirements for a service as outlined by Chandrasekaran (2015, 43-44):

a) Multitenancy: Multitenancy is an essential characteristic of cloud systems aiming to provide isolation of the different users of the cloud system (tenants) while maximizing resource sharing. It is expected that multitenancy be supported at various levels of a cloud infrastructure.
b) Service life cycle management: Cloud services are paid as per usage and can be started and ended at any time. Therefore, it is required that a cloud service support automatic service provisioning. In addition, metering and charging or billing settlement needs to be provided for services that are dynamically created, modified, and then released in virtual environments.
c) Security: The security of each individual service needs to be protected in the multitenant cloud environment; the users (tenants) also support the needed secured services, meaning that a cloud provides strict control for tenants' service access to different resources to avoid the abuse of cloud resources and to facilitate the management of CSUs by CSPs.
d) Responsiveness: The cloud ecosystem is expected to enable early detection, diagnosis, and fixing of service-related problems in order to help the customers use the services faithfully.

e) Intelligent service deployment: It is expected that the cloud enables efficient use of resources in service deployment, that is, maximizing the number of deployed services while minimizing the usage of resources and still respecting the SLAs.
f) Portability: It is expected that a cloud service supports the portability of its features over various underlying resources and that CSPs should be able to accommodate cloud workload portability (e.g., VM portability) with limited service disruption.
g) Interoperability: It is expected to have available well-documented and well-tested specifications that allow heterogeneous systems in cloud environments to work together.
h) Regulatory aspects: All applicable regulations shall be respected, including privacy protection.
i) Environmental sustainability: A key characteristic of cloud computing is the capability to access, through a broad network and thin clients, on-demand shared pools of configurable resources that can be rapidly provisioned and released. Virtualization and multitenancy technologies enables this to be achieved.
j) Service reliability, service availability, and quality assurance: CSUs demand for their services end-to-end quality of service (QoS) assurance, high levels of reliability, and continued availability to their CSPs.
k) Service access: A cloud infrastructure is expected to provide CSUs with access to cloud services from any user device. It is expected that CSUs have a consistent experience when accessing cloud services.
l) Flexibility: It is expected that the cloud service be capable of supporting multiple cloud deployment models and cloud service categories.
m) Accounting and charging: It is expected that a cloud service be capable to support various accounting and charging models and policies.
n) Massive data processing: It is expected that a cloud supports mechanisms for massive data processing.

2.3 Cloud security

Current-state architecture, engineering and operational practices in the cyber security domain focus largely on compliance to one or many regulations, directives, policies or frameworks. Security responsibilities is a major issue in cloud computing and thus is shared across the stack (Muckin & Fitch, 2015).

Data sharing in the cloud is a big risk itself. Marinescu argues that “the economical, social, ethical, and legal implications of this shift in technology, in which users rely on services provided by large data centers and store private data and software on systems they do not control, are likely to be significant” (2013, 1).

The client company uses private PaaS on a public cloud, and thus the cloud provider is responsible for security of the platform, while the consumer is responsible for everything they implement including configurations of security devices that have been offered.

Figure 7 below shows the security responsibilities while using cloud services.

Figure 7: Security responsibility in cloud services (Mogull et al. 2017, 21)

It can thus be deducted that the consumer has more security responsibilities when using IaaS while the opposite is true while using SaaS. Platform as a Service (PaaS) offers shared responsibilities between the consumer and service provider.

As outlined by the Cloud Security Alliance, "the most important security consideration is knowing exactly who is responsible for what in any given cloud project" (Mogull et al. 2017, 21).

2.3.1 Threats

"Threats, defined as people or events, are what causes damages to assets and systems in an organization. Therefore, threats must be the primary driver of a well-designed and properly defended application, system, mission, environment or enterprise" (Muckin & Fitch 2015, 3).

A white paper by Lockheed Martin Corporation in 2015 titled 'A Threat-Driven Approach To CyberSecurity' provides detailed guidance that will enable organizations to place threats at the forefront of planning, design, testing, deployment and operational activities. This is due to the fact that most resources are wasted on controls that do not address actual threats, moreover, these controls effectiveness are evaluated in binary conditions. A gap is then created since there isn't a formal threat modelling and no strict adherence to compliance requirements.

Cloud Security Alliance (CSA) released a list of twelve main threats in cloud computing in the year 2016. The list was named 'The Treacherous 12 - Cloud Computing Top Threats in 2016' and ranked these threats in the order of severity per survey results.

The threats are:

i. Data Breaches
ii. Weak Identity, Credential and Access Management
iii. Insecure APIs
iv. System and Application Vulnerabilities
v. Account Hijacking
vi. Malicious Insiders
vii. Advanced Persistent Threats (APTs)
viii. Data Loss
ix. Insufficient Due Diligence
x. Abuse and Nefarious Use of Cloud Services
xi. Denial of Service
xii. Shared Technology Issues

Controls for the respective threats have been attached in Appendix 2. According to Cloud Security Alliance, the report that was presented serves as an up-to-date guide that will help cloud users and providers make informed decisions about risk mitigation within a cloud strategy.

2.3.2 Mitigations and controls

In order to identify threats and suggest controls to be put in place, threat analysis is usually conducted with two main aims:

a) To provide a clear and thorough articulation of assets, threats and attacks to facilitate relevant decision-making actions regarding risk level determination and risk management practices.
b) To select, implement, evaluate and determine gaps in security controls at the application, system, infrastructure and enterprise levels.

3 Research Methodology

Auditing is an important process that helps in threat mitigation in cloud computing by evaluating the efficiency of the controls put in place and adherence to applicable standards. It assists in monitoring internal process of the organization, procedures and usage of tools.

Gantz (2013) states that “IT auditing helps organizations understand, assess, and improve their use of controls to safeguard IT, measure and correct performance, and achieve objectives and intended outcomes. IT audits tend to be less subjective and more reliable compared to quantitative or qualitative analysis since their determinations are more binary.” This means that the controls can either be conforming or nonconforming to the criteria.

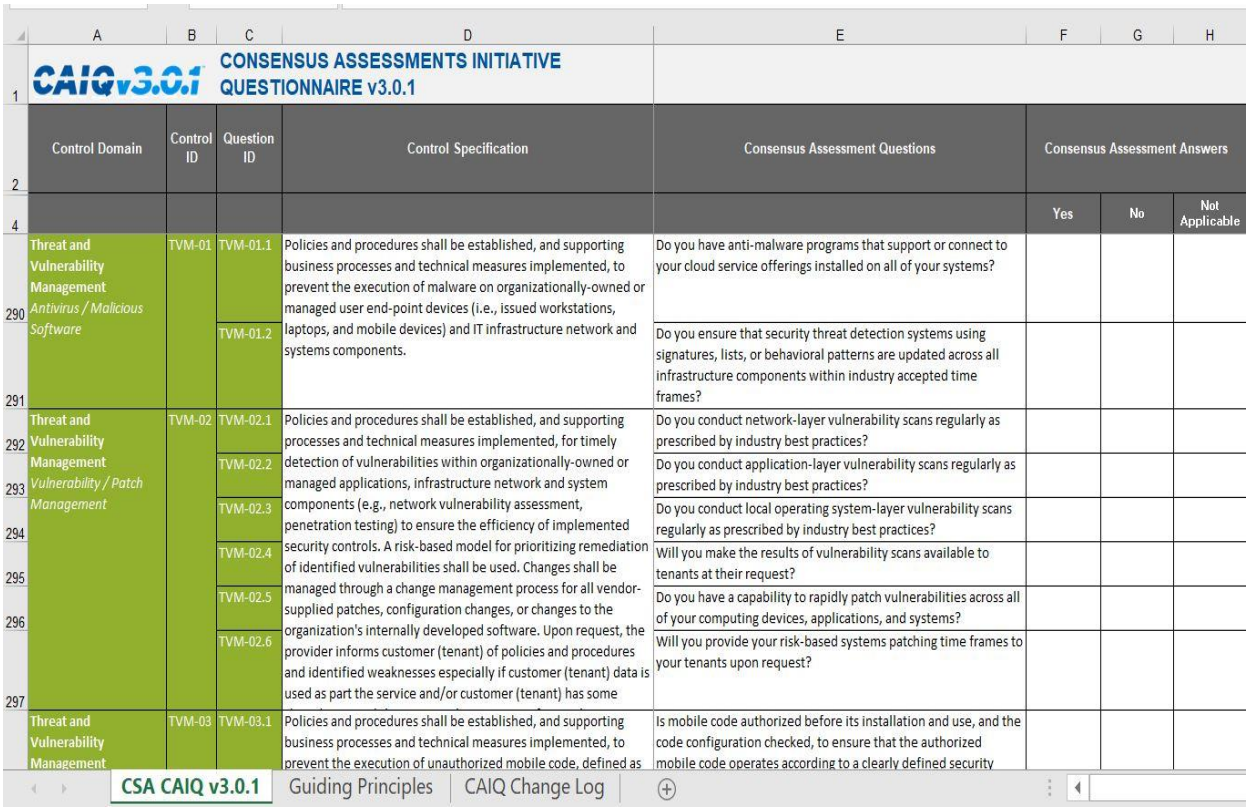
There are several reasons as to why an IT audit is justified and useful for an organization. The main reasons as justified by (Gantz 2013) are;

a. evaluating the effectiveness of implemented controls;
b. confirming adherence to internal policies, processes, and procedures;
c. checking conformity to IT governance or control frameworks and standards;
d. analyzing vulnerabilities and configuration settings to support continuous monitoring;
e. identifying weaknesses and deficiencies as part of initial or ongoing risk management;
f. measuring performance against quality benchmarks or service level agreements; and
g. self-assessing the organization against standards or criteria that will be used in anticipated external audits.

An I.T. audit was carried out to determine the scope of security measures in place, purpose of the various security controls and gaps in the implementation. Consensus Assessments Initiative Questionnaire (CAIQ) v3.0.1 by the Cloud Security Alliance was used for the audit process. The questions were tailored to suit the client company and it was based on the following elements:

a) Assessing the security controls.
b) Identifying control gaps.
c) Suggest and implement controls to fill the gaps based on the framework.
d) Managing changes over time.

A section of the Consensus Assessments Initiative Questionnaire used for the audit study is shown in Figure 8 below.



CAIQv3.0.1 CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.1

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers		
					Yes	No	Not Applicable
Threat and Vulnerability Management *Antivirus / Malicious Software*	TVM-01	TVM-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems?			
		TVM-01.2		Do you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components within industry accepted time frames?			
Threat and Vulnerability Management *Vulnerability / Patch Management*	TVM-02	TVM-02.1	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?			
		TVM-02.2		Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?			
		TVM-02.3		Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?			
		TVM-02.4		Will you make the results of vulnerability scans available to tenants at their request?			
		TVM-02.5		Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?			
		TVM-02.6		Will you provide your risk-based systems patching time frames to your tenants upon request?			
Threat and Vulnerability Management	TVM-03	TVM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security			

CSA CAIQ v3.0.1 | Guiding Principles | CAIQ Change Log

Figure 8: A section of the audit questions on CAIQ. (CAI 2016e)

Assess security controls

In many IT audits, assessment of security controls is vital since information and assets need to be protected from harm due to loss of CIA. The CAIQ questions required binary answers (yes/no) or not applicable (N/A); in the case where a question does not relate to the client or the client doesn't know whether the criteria is fulfilled.

Identify control gaps

This is done by analyzing the answers in the Consensus Assessments Initiative Questionnaire (CAIQ). The audit results is checked against the recommended control framework legislations by Cloud Security Alliance (CSA) and the gaps are therefore identified.

Suggest and implement controls

Controls that have not been implemented or partially implemented are then suggested to be replaced by controls proposed in the CSA framework.

Managing changes over time

It is important for the controls to be reviewed and new security measures implemented/updated regularly due to the evolving nature of cloud-based threats and technology in the computing world.

Five control domains were tested for compliance in the audit. These areas are:

a) Audit Assurance & Compliance
   This was to test whether the organization was compliant with the regulations for cloud deployments. Compliance validates awareness of and adherence to corporate obligations such as policies, contracts and applicable laws whereas audits are a key tool for proving/disproving compliance.

b) Business Continuity Management & Operational Resilience
   The main aspect of this section was to check whether there is continuity and recovery plan in case of a disaster.

c) Governance and Risk Management
   Governance checks the policy, process, and internal controls that comprise how an organization is run. Contracts, cloud provider assessments and compliance reporting are the key tools for governance. Risk management covers either risk to information or the organization as a whole.

d) Security Incident Management, E-Discovery & Cloud Forensics
   This domain checks whether there are policies and procedures established to check whether there is contractual obligations for employees to report information security events in a timely manner.

e) Threat and Vulnerability Management
   This is a cycle that involves threat identity, assessment, classification, remediation, and mitigation of security weaknesses while understanding the root cause analysis.

3.1 Data collection and analysis

Questionnaire and in-depth interview were the main data collection methods for the audit. An in-depth interview was conducted with the head of IT and the organization's principle, who is also the owner. During this interview questions from the CAIQ were asked and the results recorded. Data concerning the provider was also recorded and if the client didn't have an answer or was confidential was marked as 'N/A', otherwise the result was 'Yes' or 'No'.

A business impact analysis (BIA) predicts the consequences of disruption of a business function and process and gathers information needed to develop recovery strategies. Analysis of the recorded data was done by performing a business impact analysis (BIA). This is because a BIA enables the management to make important decisions during disaster recovery planning. Critical assets and areas that need immediate attention can be attended to in a timely manner, thereby saving the company in terms of finances and resources.

A qualitative risk analysis was further employed and values low, medium and high were used to evaluate the operational impact. However, the only drawback with this type of assessment was that since the scale level wasn't refined, the difference between levels aren't clearly seen.

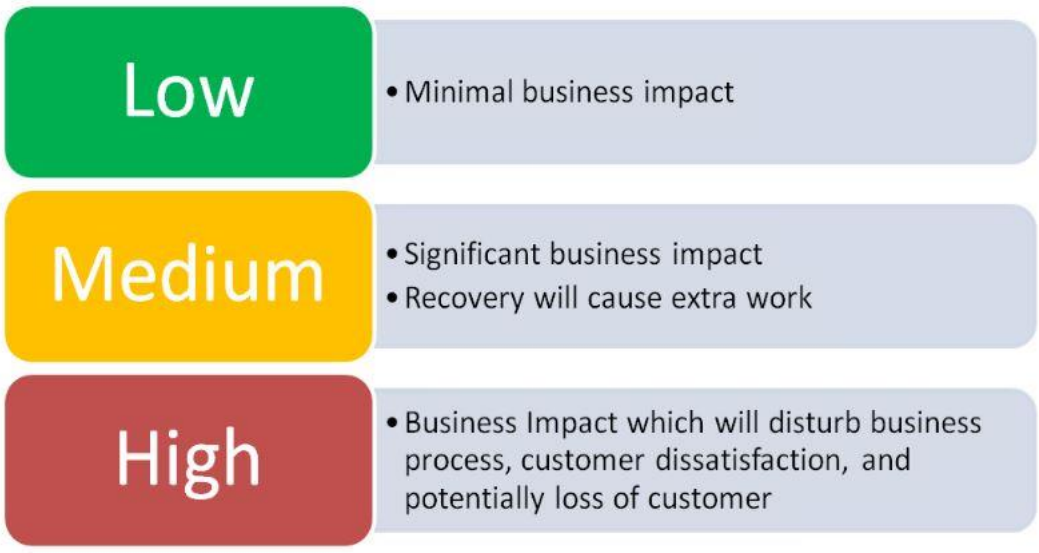


Figure 9: Qualitative analysis method (Hotchkiss 2010)

4 Audited Environment

The client company uses private PaaS (Platform as a Service) which is highlighted in yellow in Figure 10 below. In a PaaS architecture, the vendor manages infrastructure and the application stack while the client deploys onto the cloud infrastructure acquired applications and configures the user details such as logins. PaaS services are available from the internet and thus the consumer doesn't manage the underlying cloud infrastructure.

As demonstrated by Kavis (2014, 38) Figure 11 shows what cloud stacks the client manages in a PaaS architecture.

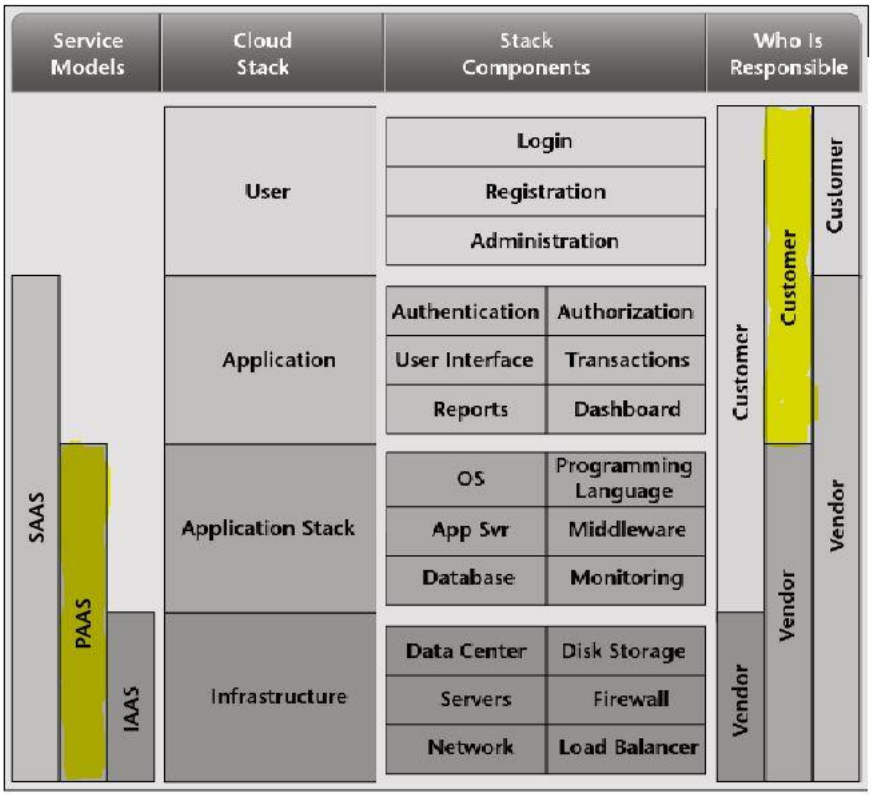


Figure 10: PaaS architecture on a cloud stack (Kavis 2014, 38)

The diagram below shows the platform that the client organization uses on a public cloud and its various essential characteristics.

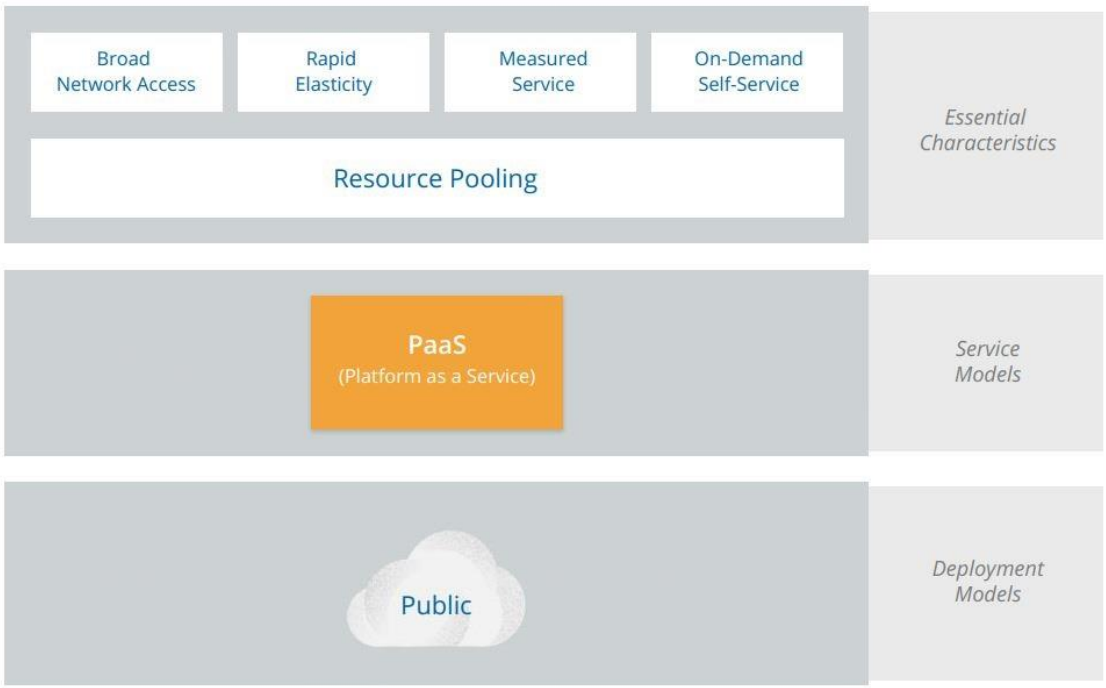


Figure 11: Client organization using PaaS on a public cloud

5 Audit Results

The Consensus Assessments Initiative Questionnaire (CAIQ) was filled out during the audit process and the detailed results are attached in Appendix 1. The results from the questionnaire was summarized as below with the respective numbers of passed, failed and N/A in different domains.

	CAIQ Results		
Domain	Yes	No	N/A
Audit Assurance & Compliance	2	5	0
Business Continuity Management & Operational Resilience	2	0	0
Governance and Risk Management	6	8	3
Security Incident Management, E-Discovery & Cloud Forensics	4	1	2
Threat and Vulnerability Management	4	4	0
Total	**18**	**18**	**5**

Table 2: Summarized results in table form

A total of 41 questions were assessed and the pass rate was a total of 18 sub-controls, failed 18 and the answers for 5 sub-controls were either confidential or not available.

Pie chart visualization of the passed, failed and “N/A” controls.

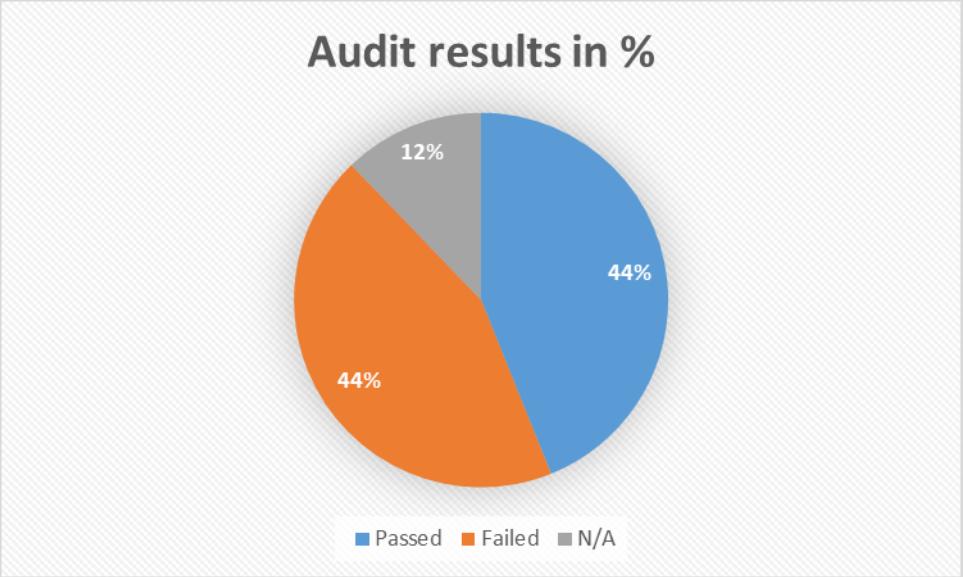


Figure 12: Pie chart of passed vs failed controls in percentage form

Based on the results of the audit, 44% of the sub controls are non-compliant with the standard framework while 44% are compliant.

The audited assets that had been marked as “No” on the CAIQ were then classified as critical or non-critical with operational impacts noted.

For operational impacts, the values were:

- Low: Operational impact is low and the business will run but may need extra re-sources.
- Medium: Business impact is significant and operations may be difficult to go on even with extra resources.
- High: High operational impact on the business which will cause financial losses and dissatisfaction within clients. Recovery may be uncertain.

Table 3 below shows the qualitative analysis of operational impact on various controls that were not in compliant with the industry standards.

Control Domain	Consensus Assessment Question not passed	Critical	Non-Critical	Operational Impact	Risk Level
Audit Assurance & Compliance	Production of audit assertions using a structured format		X	Low	5
	Conducting network penetration tests	X		High	100
	Conducting application penetration tests	X		High	100
	Conducting external audits		X	Low	5
	Internal audit program that allows for cross-functional audit of assessments		X	Medium	25
Governance and Risk Management	Capability to continuously monitor and report the compliance of your infrastructure against your information security baselines		X	Medium	25
	Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?		X	Low	5
	Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status)?		X	Medium	25
	Do you ensure your providers adhere to your information security and privacy policies	X		High	100
	Do you have agreements to	X		High	100

	ensure your providers adhere to your information security and privacy policies?				
	Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?	X		High	100
	Documented, organization-wide program in place to manage risk		X	High	100
	Do you make available documentation of your organization-wide risk management program?		X	Medium	25
Security Incident Management, E-Discovery & Cloud Forensics	Have you tested your security incident response plans in the last year?	X		High	100
Threat and Vulnerability Management	Update of security threats detection system	X		High	100
	Conducting network-layer vulnerability scans regularly	X		High	100
	Conducting application-layer vulnerability scans regularly	X		High	100
	Capability to rapidly patch vulnerabilities across all computing devices, applications, and systems	X		High	100

Table 3: Business impact analysis of the non-compliant standards

A semi-quantitative risk assessment method was used to calculate risk level. This type of assessment employs the advantages of both qualitative and quantitative analysis where qualitative analysis would be too general in classification during I.T. audits and quantitative analysis would be too extreme. “Semi-quantitative risk assessment is generally used where one is attempting to optimize the allocation of available resources to minimize the impact of a group of risks under the control of one organization” (Semi-quantitative risk characterization n.d.).

The operational impact was divided into 3 categories; Low, Medium and High. The categories were then assigned values (10 – low, 50 – 100 medium - high). In Table 4 below, the criticality level was then assigned values (1.0 - critical) and (0.5 – non-critical). The risk level was calculated by multiplying the criticality level by operational impact.

Risk level = Criticality level X Operational impact

	Operational impact		
Criticality level	Low (10)	Medium (50)	High (100)
Critical (1.0)	(1.0x10=10) Low	(1.0x50=50) Medium	(1.0x100=100) High
Non-Critical (0.5)	(0.5x10=5) Low	(0.5x50=25) Medium	(0.5x100=50) Medium

Table 4: Risk level matrix

The scale for the risk level was 0-10 low, 11-50 medium and 51-100 High.

Based on the results of the semi-quantitative analysis of the operational impact, the number of sub-controls in various risk levels is summarized below.

	(Low Risk)	(Medium Risk)	(High Risk)
Control Domains	Number of sub-controls in their respective risk categories		
Audit Assurance & Compliance	2	1	2
Governance and Risk Management	1	3	4
Security Incident Management, E-Discovery & Cloud Forensics	0	0	1
Threat and Vulnerability Management	0	0	4
Total number of sub-controls in the risk level	**3**	**4**	**11**

Table 5: Analysis of the risk level

From the results presented above in the analysis risk level, eleven sub-controls pose the highest risk level for the organization which is 100. This means that in the event of a disaster, the recovery of the organization may be uncertain and it will incur financial losses.

6 Recommendations

High risk operational impact:
Based on the results of the risk analysis level, the organization should implement a vulnerability management program to fix the non-compliant controls in Threat and Vulnerability Management domain. This is because most of the sub-controls that have a high risk level fall under this domain. In the event of a disaster, the inability of the controls to conform to the laid out industry standards will results in uncertain recovery of the organization. The primary objectives of vulnerability management according to Kandek (2015, 10) are to:

- Maintain a database of the computers and devices of your network – your hardware assets.
- Compile a list of installed software – your software assets.
- Change a software configuration to make it less susceptible to attack.
- Identify and fix faults in the installed software that affect security.
- Alert to additions of new devices, ports or software to the databases to allow an analysis of the changed attack surface and to detect successful attacks.
- Indicate the most effective workflow for patching and updating your devices to thwart attacks (such as malware, bots and so on).
- Enable the effective management of security risks.
- Document the state of security for audit and compliance with laws, regulations and business policy.
- Continually repeat the preceding steps so as to ensure the ongoing protection of your network security.

There are seven objectives that the organization should fulfil for a successful vulnerability management program:

a) Discovering and categorization of assets.
   The organization should update its current asset inventory and categorize them in groups.
b) Prioritizing assets based on risk level.
   Categorizing assets based on risk level helps in vulnerability scan customizations and assists in assigning risk rankings.
c) Vulnerability scanning.
   Perform the scan to test and analyze systems and services for known vulnerabilities.
d) Prioritizing vulnerabilities.
   After the scan, a report is generated that contains the prioritized list of vulnerabilities, vulnerability description, calculated risk, and remediation activities.

e) Generate attack paths to high risk assets.
   Attack paths helps understand where the critical assets are and how the topography around the assets look like. This assists in defining what points should be locked down in case of a severe threat.
f) Remediation, patching and monitoring.
   Remediation should be prioritized on a risk basis and should be done by the following methods:
   - Installation of a software patch
   - Adjustment of a configuration setting
   - Removal of affected software
   - Implementation of compensation control

   Patches must then be applied and monitored.
g) Validation of reports to ensure the vulnerabilities have been addressed.
   Rescanning should be done to confirm that the vulnerabilities have been addressed and reports produced to identify compliance in the ongoing security activities.

Medium risk operational impact:
Non-compliant controls that fall under Business Continuity Management and Governance pose medium risk operational impact on the organization. The organizations should change management policies to monitor changes in the organization's use of the cloud services. This should enable them to track any changes or abnormalities in their services. They should also aim to pursue a negotiated Service Level Agreement (SLA) with the cloud provider when the current one expires. This is because a negotiated SLA will enable the organization to address its security and privacy policies, compliance with laws and regulations, segregation and data encryption, breach notification and data ownership.

Low risk operational impact:
The management should undertake compliance, audits and assurance continuously to effectively manage controls that had a low risk business impact.

Detailed recommendations that should be applied as highlighted by the Cloud Security Alliance (CSA) in their 'Security Guidance for Critical Areas of Focus in Cloud Computing' document have been attached in Appendix 3.

7 Conclusion

The aim of the study was to carry out a security audit on a certification and training center for both local and international exams that uses a Platform as a Service model. Sub-controls under 5 domains were audited for compliance. The pass rate was 44%, fail was 44% and 12% was 'N/A' which means the answers were confidential or the auditee didn't know the answer. These results reflect the state of the company's IT security and systems at the time of the audit. A total of 41 questions were asked during the audit and 18 resulted in 'Yes' which means that they were compliant, 18 were marked as 'No' and 5 questions as 'N/A'. A business impact analysis was carried out on 18 controls which were failed and a qualitative analysis methodology was used to determine the level of criticality for each sub-control. A semi-quantitative analysis was then used to calculate the risk level, and this resulted 11 controls having a high risk level, 4 medium risk and 3 low risk.

A threat vulnerability management program was proposed for the high risk controls, change of policies in the organization for the medium risk controls and undertaking of compliance and audits continuously to manage low risk controls.

Decreasing expense and expanding productivity are the attracting factors for the migration towards a public cloud, yet giving up duty regarding security ought not to be. Ultimately, the organization is responsible for the decision of public cloud and the security and protection of the outsourced services. Observing and tending to security issues that emerge stay in the domain of the organization, as does oversight over other essential issues such as execution and information protection. Due to the security challenges brought about by cloud computing, it is important for an organization to oversee and manage how the cloud provider secures and maintains the computing environment and ensures data is kept secure.

Due to the evolving nature of the cloud computing world, it is important for the organization to carry out security audits regularly so that they could be compliant and be able to manage future threats effectively.

References

Chandrasekaran, K. 2015. Essentials of cloud computing. New York: Taylor & Francis Group.

Gantz, S. & Maske, S. 2014. The basics of IT audit: purposes, processes, and practical information. Waltham: Elsevier Inc.

Gregory, P. 2015. Getting and information security job for dummies. Hoboken, John Wiley & Sons, Inc.

Kandek, W. 2015. Vulnerability management for dummies, 2nd edition. Chichester, John Wiley & Sons, Inc.

Kavis, M. 2014. Architecting the cloud. New Jersey: John Wiley & Sons, Inc.

Marinescu, D. 2013. Cloud computing theory and practice. Waltham: Elsevier Inc.

Electronic sources:

Alani, M. 2014. Securing the cloud: threats, attacks and mitigation techniques. Accessed 24 March 2018.
https://www.sciencepubco.com/index.php/JACST/article/view/3588/1437

Cloud technical report. 2012. Accessed 23 March 2018.
https://www.itu.int/dms_pub/itu-t/opb/fg/T-FG-CLOUD-2012-P1-PDF-E.pdf

Data to information. 2014. Accessed 16 March 2018.
http://www.d2ikenya.com/

Hotchkiss, S. 2010. Business Continuity Management: A Practical Guide. Swindon: British Informatics Society Ltd. Accessed 21 May 2018.
https://ebookcentral.proquest.com/lib/Laurea/reader.action?docID=634527&query=

Mell, P. & Grance T. 2011. The NIST definition of cloud computing. Accessed 25 March 2018.
https://csrc.nist.gov/publications/detail/sp/800-145/final

Mogull, R., Arlen, J., Gilbert, F., Lane, A., Mortman, D., Peterson, G., & Rothman, M. 2017. Security guidance for critical areas of focus in cloud computing. Accessed 3 April 2018.
https://cloudsecurityalliance.org/download/security-guidance-v4/

Muckin, M. & Fitch, S. 2015. A threat-driven approach to cyber security. Accessed 5 April 2018.
https://lockheedmartin.com/content/dam/lockheed/data/isgs/documents/Threat-Driven%20Approach%20whitepaper.pdf

NIST cloud computing security reference architecture. 2011. Accessed 19 March 2018.
https://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/CloudSecurity/NIST_Security_Reference_Architecture_2013.05.15_v1.0.pdf

Shirey, R. 2000. Internet security glossary. Accessed 16 March 2018.
https://www.ietf.org/rfc/rfc2828.txt

The treacherous 12 - cloud computing top threats in 2016. 2016. Accessed 26 March 2018.
https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf

Journals:

Cloud compliance. 2018. Accessed 14 March 2018.
https://www.techopedia.com/definition/30551/cloud-compliance

Semi-quantitative risk characterization. No date. Accessed 26 May 2018
http://www.fao.org/docrep/012/i1134e/i1134e04.pdf

Figures

Tables

Appendixes

Appendix 1: CAIQ results

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Yes	No	N/A
Audit Assurance & Compliance *Audit Planning*	AAC-01	AAC-01.1	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.	Do you produce audit assertions using a structured, industry accepted format (e.g., CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?		**No**	
	AAC-02	AAC-02.2		Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?		**No**	
		AAC-02.3		Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?		**No**	

		AAC-02.4		Do you conduct internal audits regularly as prescribed by industry best practices and guidance?	**Yes**		
		AAC-02.5		Do you conduct external audits regularly as prescribed by industry best practices and guidance?		**No**	
		AAC-02.8		Do you have an internal audit program that allows for cross-functional audit of assessments?		**No**	
Business Continuity Management & Operational Resilience *Business Continuity Testing*	BCR-02	BCR-02.1	Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	**Yes**		
	BCR-10	BCR-10.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appro-	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	**Yes**		

			priate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.				
Governance and Risk Management *Risk Assessments*	GRM-02	GRM-01.2	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that comply with applicable legal, statutory, and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and	Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?		**No**	
		GRM-01.3		Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?		**No**	

			procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and authorized based on business needs.				
	GRM-02	GRM-02.1	Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following: • Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure • Compliance with defined retention periods and end-of-life disposal requirements • Data classification and protection from unauthorized use, access, loss, destruction, and falsification	Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status)?		**No**	
		GRM-02.2		Do you conduct risk assessments associated with data governance requirements at least once a year?	**Yes**		

Governance and Risk Management *Management Program*	GRM-04	GRM-04.1	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business: • Risk management • Security policy • Organization of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?			**N/A**
		GRM-04.2		Do you review your Information Security Management Program (ISMP) at least once a year?	**Yes**		

			• Information systems acquisition, development, and maintenance				
Governance and Risk Management *Management Support / Involvement*	GRM-05	GRM-05.1	Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.	Do you ensure your providers adhere to your information security and privacy policies?		**No**	
Governance and Risk Management *Policy*	GRM-06	GRM-06.1	Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be	Do your information security and privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?	**Yes**		
		GRM-06.2		Do you have agreements to ensure your providers adhere to your in-		**No**	

			authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.	formation security and privacy policies?			
		GRM-06.3		Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards?			**N/A**
		GRM-06.4		Do you disclose which controls, standards, certifications, and/or regulations you comply with?			**N/A**
Governance and Risk Management *Business / Policy Change Impacts*	GRM-08	GRM-08.1	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.	Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?	**Yes**		
Governance and Risk Management *Policy Reviews*	GRM-09	GRM-09.1	The organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or				
		GRM-09.2		Do you perform, at minimum, annual reviews to your privacy and security policies?	**Yes**		

			regulatory compliance obligations.				
Governance and Risk Management *Assessments*	GRM-10	GRM-10.1	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	**Yes**		
		GRM-10.2		Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?		**No**	
Governance and Risk Management	GRM-11	GRM-11.1	Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be es-	Do you have a documented, organization-wide program in place to manage risk?		**No**	

Program		GRM-11.2	tablished and documented in accordance with reasonable resolution time frames and stakeholder approval.	Do you make available documentation of your organization-wide risk management program?		**No**	
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Management*	SEF-02	SEF-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.	Do you have a documented security incident response plan?	**Yes**		
		SEF-02.3		Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	**Yes**		
		SEF-02.4		Have you tested your security incident response plans in the last year?		**No**	
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Reporting*	SEF-03	SEF-03.1	Workforce personnel and external business relationships shall be informed of their responsibility and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or	Does your security information and event management (SIEM) system merge data sources (e.g., app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?	**Yes**		
		SEF-03.2		Does your logging and monitoring framework allow isolation of an incident to specific tenants?	**Yes**		

			regulatory compliance obligations.				
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Response Legal Preparation*	SEF-04	SEF-04.1	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?			**N/A**
		SEF-04.2		Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?			**N/A**
Threat and Vulnerability Management *Antivirus / Malicious Software*	TVM-01	TVM-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems?	**Yes**		
		TVM-01.2		Do you ensure that security threat detection systems using signatures, lists, or behavioral patterns are		**No**	

			workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	updated across all infrastructure components within industry accepted time frames?			
Threat and Vulnerability Management *Vulnerability / Patch Management*	TVM-02	TVM-02.1	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?		**No**	
		TVM-02.2		Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?		**No**	
		TVM-02.3		Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	**Yes**		
		TVM-02.5		Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?		**No**	

			provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.				
Threat and Vulnerability Management *Mobile Code*	TVM-03	TVM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?	**Yes**		
		TVM-03.2		Is all unauthorized mobile code prevented from executing?	**Yes**		

Appendix 2: CSA controls

Threat	Domain	Control IDs
Data Breaches	Domain 5: Information Management and Data Security Domain 10: Application Security Domain 11: Encryption and Key Management Domain 12: Identity, Entitlement and Access Management Domain 13: Virtualization	AIS-04: Application & Interface Security – Data Security/Integrity CCC-02: Change Control & Configuration Management – Outsourced Development DSI-02: Data Security & Information Lifecycle Management – Data Inventory/Flows DSI-05: Data Security & Information Lifecycle Management – Information Leakage DSI-06: Data Security & Information Lifecycle Management – Non-Production Data DSI-08: Data Security & Information Lifecycle Management – Secure Disposal EKM-02: Encryption & Key Management – Key Generation EKM-03: Encryption & Key Management – Sensitive Data Protection EKM-04: Encryption & Key Management – Storage and Access GRM-02: Governance and Risk Management – Data Focus Risk Assessments GRM-10: Governance and Risk Management – Risk Assessments HRS-02: Human Resources – Background Screening HRS-06: Human Resources – Mobile Device Management IAM-02: Identity & Access Management – Credential Lifecycle/Provision Management

		IAM-04: Identity & Access Management – Policies and Procedures IAM-05: Identity & Access Management – Segregation of Duties IAM-07: Identity & Access Management – Third Party Access IAM-09: Identity & Access Management – User Access Authorization IAM-12: Identity & Access Management – User ID Credentials IVS-08: Infrastructure & Virtualization Security – Production/Non-Production Environments IVS-09: Infrastructure & Virtualization Security – Segmentation IVS-11: Infrastructure & Virtualization Security – Hypervisor Hardening SEF-03: Security Incident Management, E-Discovery & Cloud Forensics – Incident Reporting STA-06: Supply Chain Management, Transparency and Accountability – Third Party Assessment
Weak Identity, Credential and Access Management	Domain 11: Encryption and Key Management Domain 12: Identity, Entitlement, and Access Management	IAM-01: Identity & Access Management – Audit Tools Access IAM-02: Identity & Access Management – Credential Lifecycle / Provision Management IAM-03: Identity & Access Management – Diagnostic / Configuration Ports Access IAM-04: Identity & Access Management – Policies and Procedures IAM-05: Identity & Access Management – Segregation of Duties IAM-06: Identity & Access Management – Source Code Access Restriction

		IAM-07: Identity & Access Management – Third Party Access IAM-08:Identity & Access Management – Trusted Sources IAM-09: Identity & Access Management – User Access Authorization IAM-10: Identity & Access Management – User Access Reviews IAM-11: Identity & Access Management – User Access Revocation IAM-12: Identity & Access Management – User ID Credentials IAM-13: Identity & Access Management – Utility Programs Access HRS-01: Human Resources – Asset Returns HRS-03: Human Resources – Employment Agreements HRS-04: Human Resources – Employment Termination HRS-08: Human Resources – Technology Acceptable Use HRS-09: Human Resources – Training / Awareness HRS-10: Human Resources – User Responsibility
Insecure Interfaces and APIs	Domain 5: Information Management and Data Security Domain 6: Interoperability and Portability Domain 9: Incident Response Domain 10: Application Security Domain 11: Encryption and Key Management Domain 12: Identity, Entitlement and Access Management	AIS-01: Application & Interface Security – Application Security AIS-04: Application & Interface Security – Data Security/Integrity IAM-08: Identity & Access Management – Trusted Sources IAM-09: Identity & Access Management – User Access Authorization
System and Application Vulnerabilities	Domain 1: Cloud Computing Architectural Framework	AIS-01:Application & Interface Security – Application Security AIS-02: Application & Interface Security – Customer Access Require-

	Domain 2: Governance and Enterprise Risk Management Domain 7: Traditional Security, Business Continuity and Disaster Recovery Domain 8: Data Center Operations Domain 10: Application Security Domain 13: Virtualization	ment AIS-03: Application & Interface Security – Data Integrity AIS-04: Application & Interface Security – Data Security/Integrity BCR-04: Business Continuity Management & Operational Resilience - Documentation CCC-03: Change Control & Configuration Management - Quality Testing IVS-05: Infrastructure & Virtualization Security Management – Vulnerability Management IVS-07: Infrastructure & Virtualization Security Management – OS Hardening and Base Controls TVM-02: Threat and Vulnerability Management – Patch Management
Account Hijacking	Domain 2: Governance and Enterprise Risk Management Domain 5: Information Management and Data Security Domain 7: Traditional Security, Business Continuity and Disaster Recovery Domain 9: Incident Response Domain 11: Encryption and Key Management Domain 12: Identity, Entitlement, and Access Management	IAM-02: Identity & Access Management – Credential Lifecycle/Provision Management IAM-08: Identity & Access Management – Trusted Sources IAM-09: Identity & Access Management – User Access Authorization IAM-10: Identity & Access Management – User Access Reviews IAM-11: Identity & Access Management – User Access Revocation IAM-12: Identity & Access Management – User ID Credentials IVS-01: Infrastructure & Virtualization Security – Audit Logging/Intrusion Detection SEF-02: Security Incident Management, E-Discovery & Cloud Forensics – Incident Management

Malicious Insiders	Domain 2: Governance and Enterprise Risk Management Domain 5: Information Management and Data Security Domain 11: Encryption and Key Management Domain 12: Identity, Entitlement, and Access Management	DCS-04: Datacenter Security – Off-Site Authorization DCS-08: Datacenter Security – Unauthorized Persons Entry DCS-09: Datacenter Security – User Access DSI-04: Data Security & Information Lifecycle Management – Handling/Labeling/Security Policy DSI-06: Data Security & Information Lifecycle Management – Ownership/Stewardship EKM-02: Encryption & Key Management – Key Generation EKM-03: Encryption & Key Management – Sensitive Data Protection GRM-07: Governance and Risk Management – Policy Enforcement GRM-10: Governance and Risk Management – Risk Assessments HRS-02: Human Resources – Background Screening HRS-07: Human Resources – Roles/Responsibilities IAM-05: Identity & Access Management – Segregation of Duties IAM-01: Identity & Access Management – Audit Tools Access IAM-08: Identity & Access Management – Trusted Sources IAM-09: Identity & Access Management – User Access Authorization IAM-10: Identity & Access Management – User Access Reviews IVS-09: Infrastructure & Virtualization Security – Segmentation STA-09: Supply Chain Management, Transparency and Accountability – Third Party Audits
Advanced Persistent Threats	Domain 1: Cloud Computing Architectural	AIS-01: Application & Interface Security – Application Security

(APTs)	Framework Domain 2: Governance and Enterprise Risk Management Doman 7: Traditional Security, Business Continuity, and Disaster Recovery Domain 8: Data Center Operations Domain 10: Application Security Domain 13: Virtualization	AIS-02: Application & Interface Security – Customer Access Requirement AIS-03: Application & Interface Security – Data Integrity AIS-04: Application & Interface Security – Data Security/Integrity BCR-04: Business Continuity Management & Operational Resilience – Documentation IVS-01: Infrastructure & Virtualization Security – Audit Logging/Intrusion Detection IVS-02: Infrastructure & Virtualization Security – Change Detection IVS-05: Infrastructure & Virtualization Security Management – Vulnerability Management IVS-07: Infrastructure & Virtualization Security Management – OS Hardening and Base Controls IVS-13: Infrastructure & Virtualization Security Management – Network Architecture TVM-01: Threat and Vulnerability Management – Anti-Virus/Malicious Software TVM-02: Threat and Vulnerability Management – Vulnerability/Patch Management
Data Loss	Domain 5: Information Management and Data Security Domain 10: Application Security Domain 12: Identity, Entitlement and Access	BCR-04: Business Continuity Management & Operational Resilience – Retention Policy BCR-05: Business Continuity Management & Operational Resilience – Environmental Risks

	Management Domain 13: Virtualization	BCR-06: Business Continuity Management & Operational Resilience – Equipment Location GRM-02: Governance and Risk Management – Data Focus Risk Assessments
Insufficient Due Diligence	Domain 1: Cloud Computing Architectural Framework Domain 2: Governance and Enterprise Risk Management Domain 3: Legal Issues: Contracts and Electronic Discovery Domain 4: Compliance and Audit Management Domain 5: Information Management and Data Security Domain 6: Interoperability and Portability Domain 7: Traditional Security, Business Continuity, and Disaster Recovery Domain 8: Data Center Operations Domain 9: Incident Response Domain 10: Application Security Domain 11: Encryption and Key Management Domain 12: Identity, Entitlement, and Access Management Domain 13: Virtualization	AIS-01: Application & Interface Security – Application Security AIS-04: Application & Interface Security – Data Security / Integrity AAC-01: Audit Assurance & Compliance – Audit Planning AAC-02: Audit Assurance & Compliance – Independent Audits AAC-03: Audit Assurance & Compliance – Info. System Regulatory Mapping BCR-01: Business Continuity Management & Operational Resilience – Business Continuity Planning BCR-02: Business Continuity Management & Operational Resilience – Business Continuity Testing BCR-03: Business Continuity Management & Operational Resilience – Datacenter Utilities / Environ. Conditions BCR-04: Business Continuity Management & Operational Resilience – Documentation BCR-05: Business Continuity Management & Operational Resilience – Environmental Risks BCR-06: Business Continuity Management & Operational Resilience – Equipment Location BCR-07: Business Continuity Management & Operational Resilience – Equipment Maintenance

	Domain 14: Security as a Service	BCR-08: Business Continuity Management & Operational Resilience – Equipment Power Failures BSR-09: Business Continuity Management & Operational Resilience – Impact Analysis BCR-10: Business Continuity Management & Operational Resilience – Policy BCR-11: Business Continuity Management & Operational Resilience – Retention Policy GRM-01: Governance & Risk Management – Baseline Requirements GRM-02: Governance & Risk Management – Data Focus Risk Assessments GRM-03: Governance & Risk Management – Management Oversight GRM-04: Governance & Risk Management – Management Program GRM-05: Governance & Risk Management – Management Support/Involvement GRM-06: Governance & Risk Management – Policy GRM-07: Governance & Risk Management – Policy Enforcement GRM-08: Governance & Risk Management – Policy Impact on Risk Assessments GRM-09: Governance & Risk Management – Policy Reviews GRM-10: Governance & Risk Management – Risk Management Assessments GRM-11: Governance & Risk Management – Risk Management Framework

		IVS-06: Infrastructure & Virtualization Security – Network Security IVS-09: Infrastructure & Virtualization Security – Segmentation
Abuse and Nefarious Use of Cloud Services	Domain 3: Legal Issues: Contracts and Electronic Discovery Domain 7: Traditional Security, Business Continuity and Disaster Recovery Domain 9: Incident Response	HRS-01: Human Resources - Asset Returns HRS-02: Human Resources - Background Screening HRS-03: Human Resources - Employment Agreements HRS-04: Human Resources - Employment Termination HRS-07: Human Resources - Roles / Responsibilities HRS-08: Human Resources - Technology Acceptable Use HRS-10: Human Resources - User Responsibility SEF-01: Security Incident Management, E-Discovery & Cloud Forensics - Contact / Authority Maintenance SEF-02: Security Incident Management, E-Discovery & Cloud Forensics - Incident Management SEF-03: Security Incident Management, E-Discovery & Cloud Forensics - Incident Reporting SEF-04: Security Incident Management, E-Discovery & Cloud Forensics - Legal Preparation
Denial of Service	Domain 8: Data Center Operations Domain 9: Incident Response Domain 10: Application Security Domain 13: Virtualization Domain 14: Security as a Service	AIS-01: Application & Interface Security - Application Security BCR-08: Business Continuity Management & Operational Resilience - Equipment Power Failures GRM-01: Governance and Risk Management - Baseline Requirements IVS-04: Infrastructure Virtualization Security - Information System

		Documentation
Shared Technology Issues	Domain 1: Cloud Computing Architectural Framework Domain 5: Information Management and Data Security Domain 11: Encryption and Key Management Domain 12: Identity, Entitlement, and Access Management Domain 13: Virtualization	DSI-04: Data Security & Information Lifecycle Management – Handling/Labeling/Security Policy EKM-03: Encryption & Key Management - Sensitive Data Protection GRM-01: Governance and Risk Management - Baseline Requirements IAM-02: Identity & Access Management - Credential Lifecycle/Provision Management IAM-05: Identity & Access Management - Segregation of Duties IAM-12: Identity & Access Management - User ID Credentials IVS-01: Infrastructure & Virtualization Security - Audit Logging/Intrusion Detection IVS-09: Infrastructure & Virtualization Security - Segmentation TVM-02: Threat and Vulnerability Management - Vulnerability/Patch Management

Appendix 3: Recommendations

Domain 2 - Governance and enterprise risk management
Recommendations

- Identify the shared responsibilities of security and risk management based on the chosen cloud deployment and service model. Develop a Cloud Governance Framework/Model as per relevant industry best practices, global standards, and regulations like CSA CCM, COBIT 5, NIST RMF, ISO/IEC 27017, HIPAA, PCI DSS, EU GDPR, etc.
- Understand how a contract affects your governance framework/model.
    - Obtain and review contracts (and any referenced documents) before entering into an agreement.
    - Don’t assume that you can effectively negotiate contracts with a cloud provider—but this also shouldn’t necessarily stop you from using that provider.
    - If a contract can’t be effectively negotiated and you perceive an unacceptable risk, consider alternate mechanisms to manage that risk (e.g. monitoring or encryption).
- Develop a process for cloud provider assessments.
    - This should include:
        - Contract review.
        - Self-reported compliance review.
        - Documentation and policies.
        - Available audits and assessments.
        - Service reviews adapting to the customer’s requirements.
        - Strong change-management policies to monitor changes in the organization’s use of the cloud services.
    - Cloud provider re-assessments should occur on a scheduled basis and be automated if possible.
- Cloud providers should offer easy access to documentation and reports needed by cloud prospects for assessments.

  - For example, the CSA STAR registry.
- Align risk requirements to the specific assets involved and the risk tolerance for those assets.
- Create a specific risk management and risk acceptance/mitigation methodology to assess the risks of every solution in the space
- Use controls to manage residual risks.
  - If residual risks remain, choose to accept or avoid the risks.
- Use tooling to track approved providers based on asset type (e.g. linked to data classification), cloud usage, and management.

Domain 3 - Legal issues, contracts and electronic delivery
Recommendations

- Cloud customers should understand the relevant legal and regulatory frameworks, as well as contractual requirements and restrictions that apply to the handling of their data or data in their custody, and the conduct of their operations, before moving systems and data to the cloud.
- Cloud providers should clearly and conspicuously disclose their policies, requirements and capabilities, including all terms and conditions that apply to the services they provide.
- Cloud customers should conduct a comprehensive evaluation of a proposed cloud service provider before signing a contract, and should regularly update this evaluation and monitor the scope, nature and consistency of the services they purchase.
- Cloud providers should publish their policies, requirements and capabilities to meet legal obligations for customers, such as electronic discovery.
- Cloud customers should understand the legal implications of using particular cloud providers and match those to their legal requirements.
- Cloud customers should understand the legal implications of where the cloud provider physically operates and stores information.
- Cloud customer should decide whether to choose where their data will be hosted, if the option is available, to comply with their own jurisdictional requirements.
- Cloud customers and providers should have a clear understanding of the legal and technical requirements to meet any electronic discovery requests.

- Cloud customers should understand that click-through legal agreements to use a cloud service do not negate requirements for a provider to perform due diligence.

Domain 4 - Compliance and audit management
Recommendations

- Compliance, audit, and assurance should be continuous. They should not be seen as merely point-in-time activities, and many standards and regulations are moving more towards this model.
- Cloud providers should:
  - Clearly communicate their audit results, certifications, and attestations with particular attention to:
    - The scope of assessments.
    - Which specific features/services are covered in which locations and jurisdictions.
    - How customers can deploy compliant applications and services in the cloud.
    - Any additional customer responsibilities and limitations
  - Cloud providers must maintain their certifications/attestations over time and proactively communicate any changes in status.
  - Cloud providers should engage in continuous compliance initiatives to avoid creating any gaps, and thus exposures, for their customers.
  - Provide customers commonly needed evidence and artifacts of compliance, such as logs of administrative activity the customer cannot otherwise collect on their own.
- Cloud customers should:
  - Understand their full compliance obligations before deploying, migrating to, or developing in the cloud.
  - Evaluate a provider's third-party attestations and certifications and align those to compliance needs.
  - Understand the scope of assessments and certifications, including both the controls and the features/services covered.
  - Attempt to select auditors with experience in cloud computing, especially if pass-through audits and certifications will be used to manage the customer's audit scope.

- Ensure they understand what artifacts of compliance the provider offers, and effectively collect and manage those artifacts.
    - Create and collect their own artifacts when the provider's artifacts are not sufficient.
- Keep a register of cloud providers used, relevant compliance requirements, and current status. The Cloud Security Alliance Cloud Controls Matrix can support this activity.

Domain 5 - Information and governance
Recommendations

- Determine your governance requirements for information before planning a transition to cloud. This includes legal and regulatory requirements, contractual obligations and other corporate policies. Your corporate policies and standards may need to be updated to allow a third party to handle data.
- Ensure information governance policies and practices extend to the cloud. This will be done through contractual and security controls.
- When needed, use the data security lifecycle to help model data handling and controls.
- Instead of lifting and shifting existing information architectures take the opportunity of the migration to the cloud to re-think and re-structure what is often the fractured approach used in existing infrastructure.

Domain 9 - Incident response
Recommendations

- SLAs and setting expectations around what the customer does versus what the provider does are the most important aspects of incident response for cloud-based resources. Clear communication of roles/responsibilities and practicing the response and hand-offs are critical.
- Cloud customers must set up proper communication paths with the provider that can be utilized in the event of an incident. Existing open standards can facilitate incident communication.

- Cloud customers must understand the content and format of data that the cloud provider will supply for analysis purposes and evaluate whether the available forensics data satisfies legal chain of custody requirements.
- Cloud customers should also embrace continuous and serverless monitoring of cloud-based resources to detect potential issues earlier than in traditional data centers
    - Data sources should be stored or copied into locations that maintain availability during incidents.
    - If needed and possible, they should also be handled to maintain a proper chain of custody.
- Cloud-based applications should leverage automation and orchestration to streamline and accelerate the response, including containment and recovery.
- For each cloud service provider used, the approach to detecting and handling incidents involving the resources hosted at that provider must be planned and described in the enterprise incident response plan.
- The SLA with each cloud service provider must guarantee support for the incident handling required for the effective execution of the enterprise incident response plan. This must cover each stage of the incident handling process: detection, analysis, containment, eradication, and recovery.
- Testing will be conducted at least annually or whenever there are significant changes to the application architecture. Customers should seek to integrate their testing procedures with that of their provider (and other partners) to the greatest extent possible.

Domain 11 - Data security and encryption
Recommendations

- Understand the specific capabilities of the cloud platform you are using.
- Don’t dismiss cloud provider data security. In many cases it is more secure than building your own, and comes at a lower cost.
- Create an entitlement matrix for determining access controls. Enforcement will vary based on cloud provider capabilities.
- Consider CASB to monitor data flowing into SaaS. It may still be helpful for some PaaS and IaaS, but rely more on existing policies and data repository security for those types of large migrations.

- Use the appropriate encryption option based on the threat model for your data, business, and technical requirements.
- Consider use of provider-managed encryption and storage options. Where possible, use a customer-managed key.
- Leverage architecture to improve data security. Don’t rely completely on access controls and encryption.
- Ensure both API and data-level monitoring are in place, and that logs meet compliance and lifecycle policy requirements
- Standards exist to help establish good security and the proper use of encryption and key management techniques and processes. Specifically, NIST SP-800-57 and ANSI X9.69 and X9.73.