ENHANCED CLOUD SECURITY AND COMPLIANCE REFERENCE MODEL FOR EMERGING SAAS CLOUD SYSTEMS CONSUMING PUBLIC CLOUD SERVICES

Palamandadige Ravindu Nirmal Fernando

(199320K)

CS6997 – MSc Research Project

Department of Computer Science and Engineering

University of Moratuwa
Sri Lanka

June 2022

DECLARATION

I declare that this is my own work and this thesis does not incorporate without acknowledgement any material previously submitted for a Degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Also, I hereby grant to University of Moratuwa the non-exclusive right to reproduce and distribute my thesis/dissertation, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books).

Candidate Signature: *UOM Verified Signature*

(P.R.N Fernando)

Date: 14-06-2022

I certify that the declaration above by the candidate is accurate to the best of my knowledge and that this report is acceptable for evaluation for the CS6997 – MSc Research Project.

Supervisor Signature: . *UOM Verified Signature*

(Dr. Shantha Fernando)

Date: 16-06-2022

ABSTRACT

Most businesses in operation at present have an online presence. This ranges from an E-Commerce application to a business that offers NoSQL database capabilities as a service to its customers. With the inception of cloud computing, consumers started aligning with a service model to obtain cloud computing services. Cloud computing service models fall under three main categories: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Many businesses, especially technologically driven startups, emerge by leveraging cloud service models. Most of those emerging businesses started to offer their services as a Software as a Service model. The growth of this trend has brought up new challenges for emerging startup businesses in managing the security, compliance and privacy of their services. Compliance and privacy have been popular among cloud consumers, cloud service providers, and governments worldwide. Governments have already started taking continuous initiatives to ensure the cloud-based software services comply with the standards, and the users' privacy is guaranteed in the cloud services offered. These regulations are compulsory for a cloud business to exist in most places. If this is addressed from the perspective of an emerging SaaS business, keeping up with rapidly changing complex compliance standards and privacy regulations while making the cloud services secure has been a difficult task.

This research mainly focuses on identifying methods for creating a threat model for SaaS cloud systems and determining how cloud security and compliance make a SaaS cloud system consuming public cloud services secure and compliant. Based on that, the research proposes an enhanced reference model that consists of patterns and best practices for designing and implementing a safe, compliant SaaS cloud system. Mapping of major categories within that reference model with existing cloud security and compliance standards was also carried out to make the proposed model more relatable to the real world. An implementation phase was conducted to showcase how this proposed model can be successfully applied to the real world. This included two major components: a machine learning model and an API service. The implemented API service allows users to retrieve insights and recommendations about their SaaS system security and compliance status by responding to audit questions. The insights and recommendations were generated based on clusters identified via the implemented machine learning models. The data required to develop the machine learning model were gathered by conducting an open survey among IT professionals working or with experience working at cloud-based software solutions offering companies in Sri Lanka, the majority being startups.

This overall process paved the way for answering the research objectives while creating a solid implementation that enabled continuous and active evolvement of the proposed reference model.

Keywords: cloud computing, cloud security, cloud compliance, emerging cloud businesses, SaaS cloud systems

ACKNOWLEDGMENT

The success of this thesis depended a lot on the continuous support and guidance I received from many people. I'm incredibly privileged to have gotten this all-amazing support along with the completion of this MSc research project thesis.

I wish to thank Dr. Shahani Markus for providing me with the first insight into the main idea of this thesis and providing her guidance to make the completion of the thesis successful. I would also like to extend my sincere gratitude to Dr. Rashmika Nawarathne for his immense support for the implementation phase of this research. I would like to express my appreciation to Mr. Andun Sameera Liyagunwardana and Mr. Sachintha Rajith, my managers at Emojot (Pvt) Limited, for always supporting me and guidance in the completion of this thesis.

I owe my deep gratitude to Dr. Shantha Fernando for accepting my research title and the continuous guidance and necessary information to complete this thesis and research.

Finally, I would like to extend my deep gratitude specially to my family and friends who were always there for me and provided their full support in this endeavor.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AAC	Audit Assurance And Compliance
AIS	Application And Interface Security
BCR	Business Continuity Management & Operational Resilience
BPASS	Business Process As A Service
CAIQ	Consensus Assessments Initiative Questionnaire
Cat A – Gov	Category A – Governance
Cat A – Ops	Category A – Operations
Cat B – Gov	Category B – Governance
Cat B – Ops	CATEGORY B – Operations
Cat C – Gov	CATEGORY C – Governance
Cat C – Ops	Category C – Operations
Cat D – Gov	Category D – Governance
Cat D – Ops	CATEGORY D – Operations
CCC	Change Control & Configuration Management
CCM	Cloud Control Matrix
CCPA	California Consumer Privacy Act
CSA	Cloud Security Alliance
CSP	Cloud Service Provider
DCS	Data Center Security
DMTF-CADF	Data Format And Interface Definitions Specification – Cloud Auditing
Data Federation	
DSI	Data Security & Information Lifecycle Management
EDRM	Electronic Discovery Reference Model
EKM	Encryption & Key Management
EU	European Union
FEDRAMP	Federal Risk And Authorization Management Program
GDPR	General Data Protection Regulation
GRM	Governance & Risk Management
GSOM	Growing Self Organizing Maps
HIPAA	Health Insurance Portability And Accountability Act
HRS	Human Resources Security
IAAS	Infrastructure As A Service
IAM	Identity & Access Management
IPY	Interoperability & Portability
ISO	International Standards Organization
IVS	Infrastructure & Virtualization Security
MOS	Mobile Security
MPAA	Motion Picture Association Of America
NIST	National Institute Of Standards And Technology
OSWAP	Open Web Application Security Project
PAAS	Platform As A Service
PCI SSC	Payment Card Industry Security Standards Council
SAAS	Software As A Service
SDLC	Software Development Life Cycle
SEF	Security Incident Management, E-Disc & Cloud Forensics
SOC	Service Organization Control
SOM	Self Organizing Maps

SOX	Sarbanes–Oxley Act
STIG	Security Technical Implementation Guide
TVM	Threat & Vulnerability Management

1 – INTRODUCTION

1.1 – Background

Cloud services are expected to become an integral part of many organizations with the increase of worldwide public cloud revenue. As Gartner forecasts [1], worldwide public cloud revenue has grown by 17.5 Percent in 2019 and is expected to grow exponentially through 2022. This trend has enabled technology-driven businesses offering cloud services to emerge. The power of public cloud services has helped emerging businesses to focus on the business idea rather than worrying about their cloud services' underlying infrastructure, scalability, availability, and reliability. These services can be categorized under different cloud service models (SaaS – Software As a Service, PaaS – Platform As a Service, IaaS – Infrastructure As a Service, BpaaS – Business Process As a Service). Most emerging businesses offering cloud services fall under the cloud application services or Software as A Service (SaaS) model. According to Gartner, SaaS revenue forecasts [1] are expected to grow from 94.8 in 2019 to 143.7 in 2022 (Billions of U.S Dollars) and have the highest revenue forecast among other cloud service models justifying the growth of SaaS cloud systems.

1.2 – Cloud Security and Regulatory Compliance Standards

Cloud security and regulatory compliance standards came to the forefront since cloud computing service models were adopted to provide different services. Several standard governing bodies like CSA (Cloud Security Alliance) [2][3], NIST (National Institute Of Standards And Technology) [4], ISO (International Standards Organization) [5] etc., have developed cloud security standards. Cloud compliance came to the limelight among cloud service providers and consumers in the recent past with the European Union’s GDPR in 2019 May [6]. The newest addition to the regulatory compliance standards is the CCPA which was in effect from 2020 January [7]. Governments and regulatory bodies worldwide impose several other compliance regulations to protect user privacy and ensure personal data is secured and confidential. Though some of these regulations were in existence before cloud adoption started, now it has come to a state where businesses providing cloud services cannot neglect the importance of imposing and adhering to regulatory cloud compliance and security standards to stay in the competition.

1.3 – Problems related to cloud security and compliance standards for emerging SaaS businesses consuming public cloud services

As cloud adoption is expected to grow among consumers exponentially, cloud service providers worldwide have been facing the daunting task of ensuring their cloud services' privacy policies and user data are maintained and protected. According to Gartner [8], cloud computing tops the list of emerging risks. The executives are most concerned about the potential data risk associated with cloud computing. Most public cloud service providers create complex security and privacy controls, creating confusion among cloud consumers and providers [9]. As further expressed by Hendre and Joshi [9], this has led to a situation where cloud service providers are confused about how these controls are related to the security and compliance requirements of the business and how security controls and compliance standards are interrelated. This also includes the issue of the growing number of regulatory compliance standards. The complexity and number of regulatory compliances make the organizations struggle to implement them [10]. As further elaborated, though the organizations try to meet the requirements outlined by specific compliance standards, they haven't been able to consider all the aspects and implementation details [10]. They are prone to attacks even if they are compliant. Another critical factor that needs to be highlighted is that "compliance is not security". Though security threats are expected to evolve while regulations don't keep up with that pace [10]. These claims validate that only becoming compliant with regulatory compliance standards won't be enough without having an appropriate mechanism to identify cloud threats continuously. In the given circumstances, an emerging cloud system business would also face further issues like lack of resources, both human and financial wise, with many other practical problems to keep up with the regulatory compliance standards and security.

1.4 - Research Problem

Lack of proper cloud security and the compliance reference model for emerging SaaS cloud systems consuming public cloud services can be highlighted as the biggest issue behind the inability to keep up with the increasing complexity of the cloud's regulatory compliance standards and security standards. Most research in this area focus on cloud security and privacy standards, while others concentrated on regulatory compliance standards. Attempts to bridge the gap between the two were minimal. According to Hendre and Joshi [9], there have been

attempts to map cloud security and regulatory compliance standards. But since then, many other new and vital regulatory compliance standards like GDPR, CCPA etc., have been introduced. Also, in the scope of cloud security, many new types of threats have emerged.

A typical SaaS cloud system acts as a cloud service provider to its customers while consuming public cloud services internally to provide its services. In that case, a SaaS business should make sure they use a proper public cloud service provider that provides them with appropriate standard security controls and regulatory compliances. Also, a SaaS business should clearly understand that securing the customer data, applying identity protection and ensuring the security of application software is a responsibility that belongs to the company itself. This is often known as the Shared Responsibility Model for cloud security. A proposed model should incorporate this shared responsibility model for ensuring both cloud security and compliance.

Yimam and Fernandez present an attempt that has been undertaken to create a reference architecture or model for cloud security and compliance. Still, it hasn't been optimized for a use case focusing specifically on emerging SaaS business domains [11]. Some previous studies have attempted to map the cloud threats and existing compliance standards [9][12]. But with the addition of new types of cloud threats and compliance standards, cloud service consumers and providers are left with an open question on understanding how to map out the cloud security threats and regulatory compliance standards.

By researching the topic, I concluded that existing cloud security and compliance reference models don't focus on the practical complexities of emerging SaaS cloud systems consuming public cloud services. On top of it, existing cloud security and compliance models are getting complex and require more hands-on engagement. There wasn't any enhanced reference model specifically designed to make emerging SaaS businesses consuming public cloud services secure and compliant.

1.5 - Research Question

As the research question I have identified, *what kind of a reference model could be designed for emerging SaaS cloud systems consuming public cloud services to make their systems secure from cloud threats and compliant to cloud regulatory standards?*

1.6 – Research Objectives

This research aims to propose and build an Enhanced Cloud Security and Compliance Reference Model for emerging SaaS Cloud Systems consuming public cloud services. Considering all the different compliance standards and personal data-related issues in SaaS cloud systems, one important aspect that keeps on highlighted is the level of the security of SaaS applications. Per a comment by Troy Leach, chief technology officer at the PCI SSC, proper security standards will establish good practices that will deliver consistent results, and compliance demonstrates how well those practices are applied as expected [10]. So, increasing cloud security and putting proper controls in place will enable SaaS applications to comply with different cloud regulatory compliance standards. Also, cloud compliance would differ based on the business domain in which the SaaS operates. All the above steps would be in vain if we couldn't capture the implementation details and identify threats per each component within a cloud system. Hence enhanced methodologies need to be developed to model threats occurring within cloud systems.

A reference model like this won't be complete without having proper ways to apply and use this model successfully in the real world. Since most of the regulatory standards and reference frameworks are paper-based, much manual work is involved in completing them [13]. Also, a new model like this should be related to existing popular reference models to allow the end-users to easily showcase how they are compliant and align with controls identified in widely accepted reference models across the industry.

The following points were identified as the research objectives considering all the above factors.

- Modelling and creating a cloud security threat model for SaaS Cloud services.
- A mapping between cloud security threats and regulatory compliance standards.
- Designing enhanced cloud compliance and the security reference model for emerging SaaS cloud systems.
- Mapping the proposed enhanced cloud compliance and the security reference model for emerging SaaS cloud systems with the industry's existing and widely adopted regulatory/compliance standards and security reference models.

- Implement a practical and efficient way to use this proposed enhanced cloud compliance and security reference model successfully and conveniently in the real world for emerging SaaS cloud businesses.

1.7 – Thesis Outline

The thesis content is organized mainly based on the points discussed within the above sections.

The Literature Review chapter (Chapter 2) focuses on identifying information related to the final research outcome and validating the research problem. The initial part of the chapter focuses on deeply understanding the limitations in existing solutions or attempts which try to solve the raised research problem. Then focus shifts toward reviewing the literature required for achieving research objectives. The primary focus was on understanding the existing scope of cloud threats and cloud regulatory compliance standards while examining how they are related to the SaaS cloud delivery model. The final part of the chapter focuses on reviewing literature related to the implementation phase.

The Methodology chapter (Chapter 3) directly focuses on the core objective of this research, which is creating enhanced cloud security and the compliance reference model for emerging SaaS cloud systems consuming public cloud services. The initial part of the chapter focuses on developing a threat modelling approach designed explicitly for SaaS cloud systems. The developed threat modelling approach is a core component of the proposed reference model. The final part of the chapter focuses on developing the proposed reference model and then mapping it with an existing cloud control framework.

The Implementation chapter (Chapter 4) covers details about the final solution, which was developed to implement a practical and efficient way of using the proposed reference model. Next, the Analysis and Findings chapter (Chapter 5) discusses and presents the analysis of the testing results of the final implementation and observations made within the analysis process. Finally, the Conclusion chapter (Chapter 6) discusses the overall conclusion related to this research.

2 - LITERATURE REVIEW

The literature review has been structured based on the critical factors identified in the research objectives section. Several essential research works have been reviewed to showcase the importance of the cloud threat modelling approach. An enhanced cloud threat model approach will be an integral part of the proposed reference model for building a secure and compliant cloud system. Hence work on cloud security risks and regulatory compliance specific to the SaaS cloud has been examined (Section 2.1 - 2.4). Further extending the literature review, an analysis of the relationship between cloud security risks and regulatory compliance standards has also been carried out to identify the limitations of existing work (Section 2.5 – 2.6). In the final phase of the literature review, the focus has been put on the research work related to the implementation part of this research (Section 2.5).

2.1 – Cloud Threat Modelling

Identification of threats is a crucial way to make a system secure. As pioneers of introducing threat-based security analysis at the SDLC (Software Development Life Cycle) level itself, Microsoft has used the method of threat modelling to identify possible types of threats and security risks for their systems. As Howard claims [14], threat modelling has had the utmost importance in building secure systems from the early stages of SDLC. Another essential factor that Howard claims is that one cannot build secure systems without understanding the threats, justifying the importance of threat modelling for developing secure systems. The situation remains the same for SaaS solutions.

Initially, threat models were focused on software systems running within the on-premise infrastructure. As cloud computing emerged, new threats emerged explicitly to cloud computing. Threat driven models will ensure the security of public clouds and understand which threats exist in a cloud system [15]. Several attempts have been carried out on exploring different approaches to creating threat models for cloud computing [15][16][17]. The threat driven approach presented in [15] extends the threat model approach created by Howard - STRIDE [14]. This model has revealed threats that are common to on-premise and cloud-based resources. STRIDE-LM will specifically allow an emerging SaaS business consuming public cloud services to understand the threats associated with the data owner not owning the

underlying computing infrastructure. Urias *et al.* also present threats and mitigation tactics for each threat type in the STRIDE-LM threat modelling approach [15].

The critical elements of STRIDE-LM can be listed as,

- Spoofing
- Tampering With Data
- Repudiation
- Information Disclosure
- Denial of Services
- Elevation of privilege
- Lateral Movement

The complexity of cloud infrastructure has introduced additional threats that couldn't be identified with the STRIDE-LM threat model. These threats are mainly related to the data collected and processed using cloud systems. Securing data is a key and critical component for SaaS businesses at any level. Most regulatory compliance standards mainly focus on the data security of cloud systems. This factor has also been justified by the survey on security issues in cloud service models ranking data security as the topmost security issue in the SaaS cloud service model [18]. So, implementing a threat-driven approach only based on STRIDE-LM won't be enough for securing a SaaS cloud system. Research work carried out by Kazim and Evans brings another perspective to generalizing different types of threats specific to cloud services [16]. The particular research paper has categorized different threats for cloud services, identified possible attackers, and defined threat exploitation methodology. The main types of cloud service-specific threat types specified in [16] are listed below,

- Data breach and loss
- Evading Provenance
- Malicious Service
- Malicious Administrator
- Virtualization Threats
- Network Threats

Considering the above research work carried out related to threat modelling for cloud computing and services, the STRIDE-LM approach can be understood as the simplest and easiest threat modelling approach for emerging SaaS businesses to start their security journey. Since it consists of a set of defined components, even a small group of developers can start choosing one aspect of the threat-driven approach and begin identifying the threats to a cloud system. But STRIDE-LM alone won't allow the emerging SaaS cloud system to identify and mitigate threats completely. As proposed by Kazim and Evans, specific threat types focused on cloud service layers should also be considered in creating a cloud threat model [16].

2.2 – Security Threats for SaaS Cloud Systems

The focus of this particular section was to review cloud system threats specific to SaaS cloud systems and identify the limitations of the current work done. This section was structured based on the initial review of the most recent versions of cloud security threats identified by the standard governing bodies. It was followed by research work on cloud threat identification. Most of the research was carried out related to the main three cloud service models (IaaS, PaaS, SaaS). Since this research focuses on SaaS cloud systems, the literature review primarily focused on the SaaS cloud service model. Also, when identifying limitations of the current research work, the perspective of emerging businesses has been brought into focus.

Cloud systems have specific threats compared to threats available in on-premise systems. This has been mainly due to dynamic behaviour and lack of visibility in cloud computing. Also, cloud service consumers' lack of understanding of the shared responsibility model of cloud computing has paved the way for cloud security risks to increase. Many resources that were reviewed justified the above statement [15][16][17][19].

Multiple standard governing bodies like CSA, NIST, OSWAP, and ISO have identified different types of cloud security threats [2][3][4][5]. Critical research has been carried out to identify cloud threats [9][20]. Out of the publications done by standard governing bodies, the most significant and updated cloud threats are being recognized by CSA. The research work of CSA focused on the compilation of a precise guide defining security threats to cloud models [20]. This report has been updated regularly as new types of cloud threats emerge. Out of all

the research work reviewed, the CSA's top cloud security threats publication has been used as the basis and analysis done related to cloud threats.

Since identifying the updated and most harmful types of cloud computing threats are crucial for this research, a research study focusing on the literature publications related to cloud threats were initially reviewed. This allowed the identification of the cloud threats-related research reviewed in this literature review and verification of the credibility of the sources where threats were extracted. In doing so, 661 publications have been reviewed and classified under seven cloud computing threats identified by the CSA's "Top Threats to Cloud Computing v1.0", published in 2010. They were categorized into 15 different security domains [20].

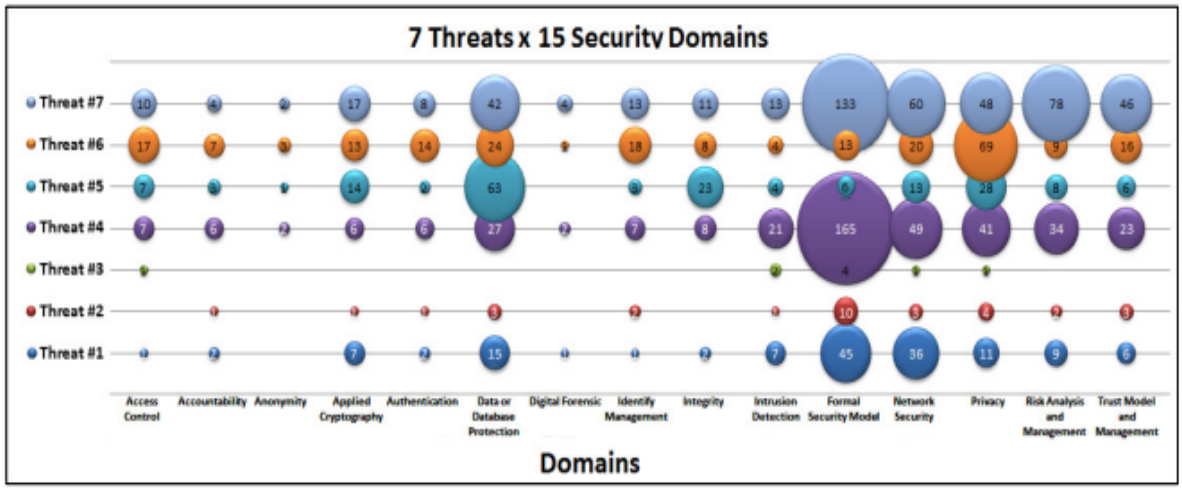


Figure 1 – Distribution of Publications by Threats and Domains as illustrated in [19, Fig. 4]

Considering the drastic changes in cloud computing over the years, the landscape of threats to cloud computing has also changed. Hence, it was crucial to identify the most recent updates related to cloud computing threats. The statement can be justified by the prediction by Gartner, stating that cloud risks have become an emerging risk to organizations [8]. Considering the above facts, the CSA's Top Threats to Cloud Computing – The Egregious 11, published in 2019, can be identified as the most recent and credible publication related to cloud computing threats [3].

Since CSA's inception, the top threat report has been created to raise awareness of the cloud's threats, risks, and vulnerabilities. The 2019 version has taken input from 241 industry experts working in the cloud security area. This version consists of 11 significant threats, risks and

vulnerabilities in the cloud environment and is ranked in the order of significance [3]. Also, each threat has been categorized under the Cloud Control Matrix [2], which is a specific set of cloud control guidelines for businesses to follow. In addition to that, each threat has been analyzed under the STRIDE threat model.

- 1 - Data Breaches
- 2 - Misconfiguration and Inadequate Change Control
- 3 - Lack of Cloud Security Architecture and Strategy
- 4 - Insufficient Identity, Credential, Access and Key Management
- 5 - Account Hijacking
- 6 - Insider Threat
- 7 - Insecure Interfaces and APIs
- 8 - Weak Control Plane
- 9 - Metastructure and Applistructure Failures
- 10 - Limited Cloud Usage Visibility
- 11 - Abuse and Nefarious Use of Cloud Services

Out of the above-ranked cloud threats, almost all the issues can be identified as essential factors for emerging SaaS businesses consuming public cloud services. Since specific challenges faced by emerging SaaS businesses in adopting security measures against these threats are not overlooked in any of the reviewed resources, it further strengthens the need and importance of research in this area. Most of the cloud threats identified here can be controlled if proper cloud security architecture and policies are put in place at the initial stages of the businesses. This can be seen as an advantage for emerging companies. But since most of those emerging businesses are focused on customer features and getting into a consistent revenue model, cloud threats often don't come into the picture in the early stages of product development and cloud architecture designing and deployment.

As per the main observations compared with the previous CSA's Top Threats report titled Treacherous 12 [21], cloud threats such as the denial of service, shared technology vulnerabilities and cloud service provider data loss and system vulnerabilities have been omitted due to their low rating. These omissions suggest that earlier cloud threats that fell under the responsibility of Cloud Service Providers (CSP) have become less concern for businesses.

This also means how well public CSPs have been trying to make their cloud services more secure. Almost all of the cloud threats identified in recent versions fall mainly under the responsibility of the cloud customer or both, while these threats reside in the higher level of the technology stack, which is the result of senior management decisions [3]. The addition of new threats to this list, such as weak control planes, metastructure and applistructure failures and limitations in cloud visibility specific to the cloud, suggests that more businesses are considering cloud migration, and the maturity of cloud consumers is increasing [3].

2.3 – Cloud Security Controls for SaaS Cloud Systems

Understanding cloud security controls were a critical factor for this research. Security controls intended to protect a cloud environment will be the same for all the cloud delivery models [9]. Cloud security controls aim to provide a framework of security standards, regulations, and rules to reduce audit complexity [2]. Identifying them will also act as a guide composed of fundamental security principles for cloud service providers.

CSA has published a set of well-identified cloud control domains. CSA claims that they use the NIST/ ISO models as its standard for defining cloud computing control domains [22]. Previous studies have been attempted and referred to as tried resources to identify cloud security control domains [2][22][9]. The CSA CCM v3.0.1 (Cloud Security Alliance – Cloud Control Matrix) publication [2] and the work carried out by Mogull *et al.* [22] identifies different types of cloud security control domains. Work published in [2] can be taken as the most updated. It introduces 16 different cloud security control domains, which are crucial when defining and mapping the compliance standards.

1. Application and Interface Security
2. Audit Assurance and Compliance
3. Business Continuity Mgmt. & Operations Resilience
4. Change Control & Configuration Management
5. Data Security & Information Lifecycle Management
6. Datacenter Security
7. Encryption & Key Management
8. Governance & Risk Management

9. Human Resources Security
10. Identity & Access Management
11. Infrastructure & Virtualization Security
12. Interoperability & Portability
13. Mobile Security
14. Security Incident Management, E-Disc & Cloud Forensics
15. Supply Chain Management, Transparency & Accountability
16. Threat & Vulnerability Management

The cloud control framework published by CSA in [2] (CSA Cloud Control Matrix) provides mapping to almost all the cloud regulatory compliance standards and frameworks worldwide, including those listed in the next section.

2.4 – Cloud Regulatory Compliance Standards and frameworks for SaaS Cloud Systems

Cloud regulatory compliance standards mainly focus on ensuring the privacy of the data of consumers that the cloud service providers are processing. The confidentiality and security of cloud data remain the primary concern for customers regarding cloud adoption from the beginning [9]. This can be justified as the data breach being the top-ranked cloud threat on all versions of CSA's Top Cloud Threat publications. Though there has been a massive increase in cloud adoption over recent years and is estimated to be growing strongly [1], the threats affecting data processing in the cloud remain the topmost cloud threat.

Regulatory compliance standards refer to the discipline and process of ensuring that a company follows the laws enforced by governing bodies [23]. These laws can be on a geographical basis or based on industry standards. As further elaborated in [23], the frequently changing nature of the regulatory compliance standards is a challenge for cloud businesses.

Previous studies [9][12] have attempted to identify major regulatory compliance standards regarding the cloud. But these attempts lack the information on newly introduced regulatory compliance standards. Two of the most recent developments in this area are GDPR and CCPA regulatory compliances standards. The impact of these on cloud businesses are enormous. GDPR is designed to protect data related to every citizen in the European Union (EU) [23], so

cloud businesses offering services to EU citizens should comply with GDPR. Stalling's study on CCPA [24] identifies it as the most influential state-level data privacy law imposed in the United States and expected to be a model for privacy laws in other states across the United States. This makes businesses operating in the United States also concerned with CCPA and existing regulatory compliance standards. According to the same source, there has been an increase in data protection laws imposed globally. GDPR is also the most complex piece of a compliance framework introduced anywhere globally, directly affecting over 500 million people [25]. It can be considered the standard for other jurisdictions worldwide when geographically implementing regulatory compliance standards [26].

Organizations that specifically handle and process different types of data fall under regulatory compliance standards, which in most cases are legally bound and carry penalties when not appropriately implemented [19]. According to NIST, organizations are fully responsible for handling compliance-related issues [27]. Understanding and enforcing regulations is a significant challenge for cloud systems due to the lack of transparency in public cloud compliance [27]. Due to that, most cloud service providers use third party certifications to confirm their compliance. Table 1 consists of significant security compliance models and frameworks that affect cloud service models identified in this literature review and remarks extracted from different sources. Based on the information, most security compliance models and frameworks are specific to other geographical areas or industries. Another essential feature among these cloud regulatory compliance standards is that they can be categorized based on the business domain of the cloud system.

Table 1 – Cloud Regulatory Compliance Standards and Remarks *(Spans across multiple pages)*

Cloud Regulatory Compliance Standards	**Remarks**
STIG (Security Technical Implementation Guide)	Enforced by the Department of Defense, USA. Specific to Federal IT Systems in the USA. Focuses on Federal IT System Infrastructure. [28]
FedRAMP (Federal Risk and Authorization Management Program)	Established to address security and reliability of cloud services used by the Federal Government. Specific to the USA. [29]

DMTF-CADF (Data Format and Interface Definitions Specification – Cloud Auditing Data Federation)	The standard which enables effective management of IT environments. It's a global standard that anyone can use to certify, manage and audit application security in the cloud. [30]
ISO-17799 (International Organization For Standards)	Provides guidelines for best practices for implementing and maintaining information security management systems. Information security is defined based on the CIA triad. [31]
ISO-27001 (International Organization For Standards)	Specifies the requirements for implementing, maintaining and information security management systems aligning with the best practices presented in ISO-17799. This is a formal standard model where organizations can seek independent certification of their ISMS. [31]
ISO 27002 (International Organization For Standards)	Renamed after ISO 17799. [31]
FIPS 140-2	Implemented by NIST, USA. Focusses on security requirements for cryptographic modules. [32]
PCI DSS	Implemented by a global governing body to ensure payment data security. [33]
HIPAA (Health Insurance Portability and Accountability Act)	Implemented by the U.S Department of Health and Human Services (HHS). The main motive behind this compliance model is to secure individually identifiable health information that is held or transferred in electronic form. [34]
SOX (Sarbanes–Oxley Act)	Enforced by the United States Congress to protect shareholders and the general public from accounting errors. SOX is most about

	financial controls, but it consists of regulations that include what kind of financial records that needs to be stored and for how long. [35]
MPAA (Motion Picture Association of America)	MPAA has established this compliance model for defining best practices for secure storing, processing and delivering protected media content. Media companies can use this standard as a way to assess the risks and security of their content and infrastructure. [36]
SOC 2	Developed by the American Institute of CPAs. It defines criteria for auditing the service providers to securely manage data of your organization to protect the interest of the organization and its clients. [37]
EDRM (Electronic Discovery Reference Model)	A framework that defines outline standards for recovery and discovery of digital data. Designed as a guide to assist the gathering of electronic data in a legal process, including criminal discovery. [38]
GDPR	Imposed by the European Union, it can be identified as the compliance standard model which affects the largest number of customers and businesses out of all the compliance models mentioned here. It also carries huge legal penalties if proper controls aren't initiated. [39]
CCPA (California Consumer Privacy Act)	Enforces more repercussions and controls to businesses operating in California. It allows consumers to demand the organization to see all the data stored about them and a full list of third parties where their data is shared. It

	also allows consumers to sue the organizations when privacy guidelines are violated, even without a breach. [40]
NIST SP 800-53	Provides an exhaustive catalog of controls designed to make federal information systems more resilient. These controls are fully operational and technical and designed to create management safeguards that can then be used by various information systems including cloud systems [41]. Though these controls are intended for federal systems, aligning with this control framework will be great way for companies to comply with regulatory standards.

When SaaS businesses provide their services in different business domains and to customers spread in a vast geographical area, a huge challenge lies ahead of them to make sure their services are compliant in the cloud with the regulatory compliance standards and the control frameworks. Also, though a SaaS business may not require being compliant with these regulatory compliance standards or frameworks, aligning with them and implementing those recommendations can be hugely beneficial to maintaining proper cloud security and compliance status.

2.5 – Mapping between Cloud Threats and Cloud Regulatory Compliance Standards for SaaS Cloud Systems

The main focus of this section was to review the relationship and mappings identified between cloud threats and cloud regulatory compliance standards in previous studies. Several previous attempts have been carried out on mapping the relationship between cloud threats and cloud regulatory compliance standards [9][12]. Multiple attempts have also been carried out on linking the impact of GDPR with cloud computing [39][42][43]. Though Stalling's study on CCPA [24] isn't directly linked with cloud computing, his insights on how personal data should be processed is an important aspect that cloud businesses need to be aware of.

Businesses operating in the SaaS domain are responsible for securing the data as customers using public cloud services and ensuring the services, platforms and infrastructure as cloud service providers to their customers [12].

The study done by Hendre and Joshi [9] presents a recommendation for a security compliance model based on different security threats. It maps out the sections that apply to each cloud threat type and the recommended security compliance model. A survey by Yimam and Fernandez presents [12] An analysis and comparison of some common types of regulatory compliance standards applicable in the United States. But as per the same study, many countries have similar kinds of regulatory compliance standards customised to their local needs, similar to GDPR applicable for EU citizens.

Table 2 - Recommendations for security compliance model based on security threats that are presented in [9, Tab. 1]

Type of threat	**Security Compliance Model**
Data breaches	STIG, FedRAMP, DMTF-CADF, ISO-27001, FIPS 140-2, PCI DSS, ISO 27002, HIPAA, SOX
Data loss	STIG, FedRAMP, DMTF-CADF, FIPS 140 -2, PCI DSS, ISO 27002, HIPAA, SOX
Account or service hijacking	STIG, FedRAMP, DMTF-OVF, ISO- 27002, FIPS 140-2, NIST 800 -61, ISO 17799
Insecure interfaces/API	OASIS and OVF, DMTF-CADF, ISO 27002, FIPS 140-2
Denial of services	PCI DSS, ISO 27001, HIPAA, SOX, NIST 800-61, ISO 17799
Malicious insiders	ISO 27002, FIPS 140-2, Vaultive, FedRAMP
Abuse of cloud services	NIST 800-61, ISO 17799, NIST 800-50
Insufficient due diligence	EDRM, NIST 800-61
Shared technology vulnerabilities	ISO 27001, FIPS 140-2, PCI DSS, ISO 27002, HIPAA, SOX, MPAA

The table 2 consists of the recommendations of the security compliance model for each threat based on CSA's top threat publication, which was based on the information extracted from the

study by Hendre and Joshi [9]. The cloud threats mentioned here are a bit outdated. Some of the compliance models here are only specific to certain business domains and primarily based only on the United States. But this categorization provided a clear idea of different mapping types of cloud threats and security compliance models.

Table 3 - Responsibilities of Cloud Consumers and Cloud Providers - Presented in [28, Tab. 1]

Cloud Consumer Responsibilities	Cloud Provider Responsibilities
Article 5: Processing of Personal Data – Personal data should be transferred in a lawful and transparent manner. It shouldn't be processed in any way where users haven't provided their consent.	**Article 28 (2-4) (10): Responsibility of Processor –** Insisting the confidentiality responsibilities and work according to the rules if sub providers are appointed.
Article 24: Responsibility of Consumer – Consumer is responsible for providing the technical and organizational measures needed for GDPR	**Article 29: Processing under the consumer authority –** All consumer data should be processed with the consent of the user, unless there are any requests by the Union or the state law.
Article 25: Data protection by Design and by Default – Data should be collected, stored and processed only for required purposes. Techniques like pseudonymization and data minimization should be applied.	**Article 37: Designation of Data Protection Officer –** DPO officer is suggested to be hired if a continuous monitoring of a data object in a large scale is done. DPO should be hired based on their expertise in privacy laws in practice.
Article 26: Joint Consumers – All consumers should be GDPR compliant	**Article 44: General Principles for Transfer** – Responsibilities related to cross-border transactions will applied to providers
Article 27: Representatives of Consumers and Providers not established in the Union – It's important to appoint a legal or natural person in the EU if a consumer or provider is outside of the EU.	
Article 34: Communication of Personal Data Breach – Customers should be notified in clear and plain language about a data breach within 72 hours.	

The study done by Elluri and Joshi [43] presents a clear knowledge representation of cloud data controls for GDPR. It identifies the main sections in GDPR documents that affect cloud computing providers and consumers and divides the GDPR articles based on cloud provider and consumer responsibility. The study [39] identifies the joint responsibility of cloud service providers and cloud service consumers in providing compliance with GDPR.

The table 3 consists of data extracted from the study by Elluri and Joshi [43], which showcases the GDPR articles related to different responsibility scopes of the cloud provider and consumers.

Though previous studies have been carried out in mapping cloud threats with regulatory compliance standards, the types of cloud threats have been updated over the years, and mapping between new kinds of cloud threats and compliance standards hasn't been done. Also, with the addition of GDPR and CCPA, mapping updated cloud threats with the latest regulatory compliance standards are essential for cloud businesses.

One can argue that most of these regulatory compliance models are primarily concerned with a specific geographical location. But as a SaaS platform offering services to global clients creating proper security controls and aligning with the expected security levels for these compliance standards are a must for business continuity. Also, since these compliance standards mainly emphasize enabling proper and rigorous security controls in place to protect consumer data and privacy, adhering to and bringing in the security best practices on those regulatory compliance standards will allow emerging SaaS businesses to make their cloud systems more secure. Complying with all the regulatory compliance standards will be a daunting and impractical task for an organization at any level, so selecting a single regulatory compliance standard and making an effort to implement security control recommendations of that compliance model will be the best way to move forward for emerging SaaS businesses.

2.6 – Reference Models on Cloud Security and Cloud Compliance

Several previous studies [44][19] have attempted to create a security model for cloud computing. A study was also done on exiting cloud security models and strategies for cloud computing in [45].

The study presented by Fawaz *et al.* [44] shows us a security model for cloud computing and an organization's responsibilities towards security governance, risk management and compliance. But the model that was presented only focused on cloud computing security and threats. The study done by Bharadwaj *et al.* [19] has come up with a cloud threat defence – security model for assessing the threats in cloud computing. Again, this model is too broad, and it only focuses on identifying cloud assets, identifying cloud threats on them and remediation those threats. A comprehensive study was done by Che *et al.* [45] on the security models and strategies of cloud computing. This study has summarised four cloud computing security models – The Cloud Multiple Tenancy Model of NIST, The Cloud Risk Accumulation Model of CSA, Jerico Forum's Cloud Cube Model, and The Mapping Model of Cloud Security and Compliance. While the first three models presented in the study focus on cloud security, the last model focuses on mapping cloud security and compliance. According The Mapping Model of Cloud Security and Compliance, to protect cloud resources effectively, we should first analyze security risks, find the gaps according to the cloud architecture and its compliance framework, and finally adopt the relevant security controls.

The CSA's Security Guidance for Critical Areas of Focus in Cloud Computing v.4.0 [22] has also presented a simple cloud security process model, which they describe as a relatively straightforward, high-level process for managing cloud security.

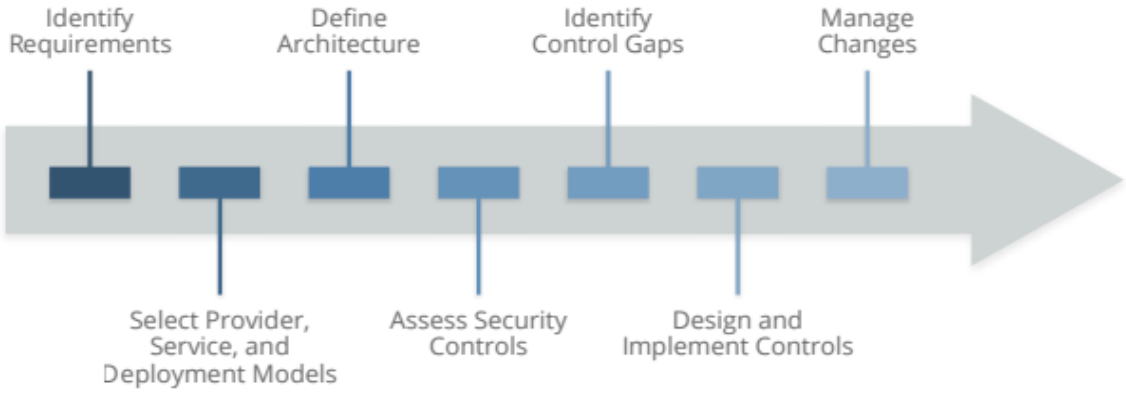


Figure 2 – A Simple Cloud Security Process Model as illustrated in [21, Section. 1.2.2.1]

SaaS cloud service provider is responsible for nearly almost all of the security. It's responsible for perimeter security, logging/ monitoring/auditing, and application security, while the SaaS cloud system consumer may only be able to manage authorization and entitlements [22]. In

most cases, since SaaS also consumes public cloud services, it makes the SaaS business itself a cloud consumer. Hence, the responsibility of cloud providers and consumers falls into a SaaS cloud system that consumes public cloud services. This is known as the Shared Responsibility Model for the cloud, which was briefly introduced earlier. CSA clearly defines the roles of a cloud provider and a consumer as stated below,

The Cloud Provider's responsibility should clearly define internal security controls and customer security features. The consumer can make decisions based on that. Providers should also correctly design and implement those controls [22].

The Responsibility of Cloud Consumer – Should build a matrix to document who is implementing which controls and how are those implemented. It should also align with the necessary compliance standards [22].

Considering all the models referred to here, none of the models has incorporated whether each step made in managing cloud security aligns with the regulatory standards. Hence, enhanced cloud security and the compliance reference model for emerging SaaS cloud systems consuming public cloud services are yet to be implemented.

2.7 – Literature review related to the implementation phase

In the initial part of this section, I had to decide the best possible way of creating an implementation capable of providing insights into an emerging SaaS business's security and compliance status based on the proposed reference model. Ensuring the implementation is practical, adaptive and easily consumable was also a vital part of deciding the idea for the implementation. Considering all those points, the decision was taken to generate a machine learning model that can predict an emerging SaaS business's security and compliance status based on the reference model proposed in this research. The central questions that had to be answered were what kind of machine learning model must be developed and what type of data must be collected and used to train that model.

Since what's proposed within this research was a reference model, the most obvious way to create a data set based on the proposed reference model was to generate a survey questionnaire

that captures respondents' answers whether they are compliant with security and compliance controls that are expected within the proposed reference model. In deciding what questions to ask to gauge a SaaS service provider's security and compliance posture, I had to base my questions on a previously verified questionnaire already in use within the real world to perform this kind of security and compliance background on cloud service providers. Based on this background, I have reviewed several once-implemented questionnaires to identify cloud service providers' security and compliance levels. Out of those, the CSA's Consensus Assessment Initiative Questionnaire (CAIQ) v3.0.1 [46] could be identified as the clearest and best questionnaire out there. It offers an industry-accepted way to document security and compliance controls in IaaS, PaaS, and SaaS services [46]. It consists of a set of Yes/No questions (dichotomous questions) a cloud consumer and a cloud auditor may wish to ask of a cloud provider to ascertain their compliance to the Cloud Controls Matrix (CCM) [2] [46]. Therefore, it helps cloud customers to gauge the security posture of prospective cloud service providers and determine if their cloud services are suitably secure [46]. In this literature review effort, I have also identified a more concise version of the CAIQ v3.0.1 (CAIQ-Lite) published by a collaborative effort between CSA and Whistic [47]. The CAIQ-Lite version consisted of only 73 questions compared to over 150 questions within the CAIQ v3.0.1. It was claimed to be reviewed by a panel of over a hundred IT security professionals [47].

Based on the proper methodology to create a survey to generate the data set for training the machine learning model, the next phase was to identify how the machine learning model could be developed. As the machine learning model's expected outcome was to predict and generate security and compliance insights for a SaaS system, a machine learning technique to identify similarities between the data points in the data set should be used. Hence, clustering the data set was selected as the machine learning technique. The idea was to identify different clusters of respondents with similar survey responses and then create a set of unique insights for each cluster. Based on this background, the motive behind the literature review part for this phase was to identify what type of clustering algorithm can be used for this scenario. In clustering, choosing the initial cluster centers is extremely important as they directly impact the final cluster formation [48]. As Cao *et al.* clearly state, clustering algorithms can be mainly categorized into two types based on the difference between the data used to cluster, either numerical data or categorical data. Hence, the clustering technique used within this scenario depends on the data type of the data set features.

The data set consists of survey questions and the responses that belong to either Yes, No or Not Applicable categories, which puts this data set under categorical type. As Cao *et al. state,* the k-modes algorithm could be identified as the algorithm which is ideal for this implementation.

2.8 – Conclusive Remarks

The main focus of the Literature Review was to identify necessary details within existing literature related to Cloud Security and Cloud Regulatory Compliance Standards, along with gathering information required for the implementation phase of the research. Initially, cloud threat modelling approaches have been looked at to get an idea of existing approaches. Then literature on cloud threats specific to SaaS cloud systems has been reviewed. Following that, cloud regulatory compliance standards for SaaS cloud systems were reviewed. Then, more focus was given to literature mapping between the cloud threats and cloud regulatory compliance standards for SaaS cloud systems. By doing so, I identified the existing models and frameworks related to cloud security and regulatory compliance standards. Also, it allowed me to identify the setbacks of existing approaches and specific details that I should give more attention to when designing and solving the research objectives. In the final phase of the literature review, I explored ways of designing the implementation and the background research related to that implementation.

3 – METHODOLOGY

The overall motive behind this research was to create enhanced cloud security and a compliance reference model for emerging SaaS cloud systems that consume public cloud services. The main components of the research objectives were identified in the Introduction chapter (Chapter 1). The Literature Review chapter (Chapter 2) allowed us to understand cloud threats and regulatory compliance standards that are constantly emerging and becoming complex. The ability to keep up with the changes is the most challenging part. This issue has been shared among all technology-related organizations [10]. The complexity will probably increase if your business is in the SaaS cloud service domain. Additionally, an emerging SaaS business faces many issues compared to a large established organization on this front as emerging SaaS businesses rely on a limited number of human resources performing different job roles. With the additional challenges and complexity of cloud threats and regulatory compliance standards, it's easy for emerging businesses to postpone acting on those issues. But continuously failing to address those would carry huge technical debts. Hence it is essential to create a proper model considering all the aspects related to cloud threats and regulatory compliance standards focusing on the emerging SaaS businesses.

Before creating the model, a comprehensive literature review was done on previous work carried out related to this area. It was categorized based on the critical points identified in the research objectives section. By doing so, I identified specific limitations of the previous research attempts and came up with solutions to improve those limitations. The methodology section was structured based on those improvements. These subsections consist of improvements identified with new additional areas that need to be looked at with the recent updates in cloud threats and regulatory compliance standards. These are essential components of a reference model that allows an emerging SaaS cloud service business to make its services secure against specific cloud threats and compliant with standard regulatory compliance standards. Following that, the enhanced cloud security and the compliance reference model for emerging SaaS cloud systems consuming public cloud services was presented (Section 3.3). With the proposed reference model in place, the methodology section next highlights the process behind identifying the major cloud control domains from CSA Cloud Control Matrix domains [2] which were filtered depending on the cloud controls associated to topmost cloud threats published in CSA's Top Threats to Cloud Computing – The Egregious 11 publication

[3]. This filtration allowed the identification of cloud controls that are associated with the top cloud threats and simplify the focus that should be put in by emerging SaaS businesses when implementing or aligning with these controls. Finally, a mapping between those filtered cloud control domains and the proposed reference model were presented. Those mappings act as the basis for the implementation part of this research (Section 3.5).

3.1 – STRIDE-LM+ - An Optimized Threat Modelling Approach for Emerging SaaS Businesses consuming public cloud services

Considering the factors in the literature review, we can conclude that the best way for an emerging SaaS business to make a complete threat-driven approach was to combine the threat modelling approaches identified. Vincent *et al.* clearly state that cloud infrastructure also consists of threats beyond STRIDE-LM [15]. The research carried out by Kazim *et al.* defines the threat model should be based on specific cloud services and data processed by services. Hence, combining those two threat model approaches will allow engineering teams working in emerging SaaS businesses to identify different types of business or domain-specific cloud threats.

A summary of threat types, possible attackers and mitigation tactics that combine both threat modelling approaches optimized for emerging SaaS Cloud System – STRIDE-LM + is presented in Table 4.

Table 4 – Summary of STRIDE-LM+ Threat Modelling *(Spans across multiple pages)*

Threat Type	**Possible Attackers**	**Mitigation Tactics**
Spoofing • Unauthorized IAM Access Privilege Change	Outside Attacker, Malicious Insider	• Securing, Monitoring and Alerting User Account Activity • Rotating User Account credentials periodically • Storing and securing audit trails of user activity in cloud.

Tampering with Data • Unauthorized Tampering, modifying cloud services or data associated with those. • Installation of malicious application which tampers data.	Outside Attacker, Malicious Insider, Malicious User	• Encrypting Data • Collecting and Encrypting Audit trails of user activity
Repudiation • Unauthorized user claiming that he/she didn't access cloud account	Malicious User, Malicious Insider	• Monitoring audit trails of user login activity.
Information Disclosure • Unauthorized File transfer occurring to/ from cloud environment. • Unauthorized egress/ ingress network connections to cloud servers from malicious connections. • Unauthorized viewing or editing critical files.	Outside Attacker, Malicious User, Malicious Insider, Cloud Service Provider	• Using encryption methods to encrypt data stores. • Encrypt secure connections. • Monitor malicious connection attempts that occurs to cloud servers and then blocking. • Define proper access roles, user groups with defined access roles and add users to those user groups. This makes managing and tracking user activity easy. • Continuously do vulnerability analysis and monitor security settings.

• Unauthorized access, view critical data stores. • Unauthorized changes to network access control lists. • Risky Cloud Configurations - Not encrypting data stores, all IP access to critical services, default security applied. • Cloud data deletion setting not applied or referred.		• Check for insecure, default security policy applied locations and resources.
Denial of Service • Denial of service against critical cloud infrastructure • Unauthorized user terminating critical cloud servers.	Outside Attacker, Malicious Insider	• Whitelisting and blocking IP addresses. • Place proper access controls for access to critical cloud services. • Enabling alerts to monitor critical cloud services.
Elevation of Privilege • Cloud User privilege escalation.	Malicious Insider, Malicious User	• Alerting enabled for cloud user privilege changes. • Use secure cloud accounts to run critical processes.

Lateral Movement • Unauthorized attempt to access or scan adjacent hosts. • Unauthorized attempts to change security groups which acts as firewall policy rules in the cloud.	Malicious Insider	• Use flow logs to analyze cloud network traffic and create alerting for invalid flows.
+		
Virtualization Threats • Cross tenant attack by sniffing or spoofing. • Installing malware to OS. • Unauthorized code execution.	Outside Attacker, Malicious User	• Impose proper access controls to operating systems. • Do periodic vulnerability analysis and server patching.
SaaS Applistructure Specific Threats • Insecure coding practices. • Network based attacks (Phishing, SQL-Injection, Cross-site	Outside Attacker, Malicious User	• Impose proper secure coding practices. • Implement secure coding review practices. • Do Application vulnerability testing periodically to identify application specific threats.

Scripting, Cross-site Forgery)		

3.2 – Threat Analysis on CSA's top threats using the STRIDE-LM+ threat model

Based on the literature review, I have found that all the research attempts in the cloud threats domain used CSA's official publication on cloud threats as the primary source for cloud threat identification. But with the most recent version of CSA's cloud threat publication [3], some of the previously identified threats were removed, and new types of cloud threats were added. This section aims to present a threat analysis on each of those updated cloud threats using the STRIDE-LM+ model.

The table 5 consists of the top most cloud threats and the threat analysis for each threat done using the STRIDE-LM+ threat model. Each threat also carries details on how they relate to emerging SaaS businesses. These details are obtained through case studies referred to and from personal experience of mine by working at an emerging SaaS business consuming public cloud services for over three years.

Table 5 – Threat Analysis using STRIDE-LM+ threat model on CSA's Top Threats to Cloud Computing - The Egregious 11 [3] ***(Spans across multiple pages)***

Cloud Threat	**Threat Analysis – STRIDE-LM+**
Data Breaches • Incidents where sensitive, protected and confidential information is released, viewed or stolen by unauthorized parties. *Most important cloud threat that emerging SaaS businesses should be aware of. Management of all the other threats in this section directly*	• Information Disclosure • SaaS Web Application Specific Threats

impacts this threat. Almost all of the regulatory compliance standards has given a key importance to data breaching activities, including GDPR and CCPA.	
Misconfiguration and Inadequate Change Control • Occurs when cloud computing assets are not configured properly. • Occurs when user logins are not properly rotated. • Access controls or permissions not properly configured. *Emerging SaaS businesses can easily go wrong with this if they lack services of an experienced cloud engineer who has familiarity with cloud computing configurations. Since most of the emerging businesses focus on quickly deploying their products to the customers, there is a high risk where proper cloud-based configurations are done. If they aren't aware of those they tend to move along with these misconfigurations.*	• Tampering with Data • Repudiation • Information Disclosure • Denial of Service • Lateral Movement • Virtualization Threats • SaaS Web Application Specific Threats
Lack of Cloud Security Architecture and Strategy	• Spoofing Identity • Tampering with Data • Repudiation • Information Disclosure

This would be affecting the same way when a large organization migrating their workloads to cloud or an emerging business who are starting off with cloud computing without any cloud security architecture or strategy in place.	• Denial of Service • Elevation of Privilege • Lateral Movement • Virtualization Threats • SaaS Web Application Specific Threats
Insufficient Identity, Credential, Access and Key Management *Emerging SaaS businesses would face this situation if proper identity access management processes are not defined. It will pave the way for unauthorized parties to easily access the system and perform unauthorized tasks.*	• Spoofing Identity • Tampering with Data • Repudiation • Information Disclosure • Denial of Service • Elevation of Privilege • Lateral Movement • Virtualization Threats • SaaS Web Application Specific Threats
Account Hijacking *Highest risks for these types of security issues are cloud service and subscription accounts which controls billing. Account breach or hijacking can provide access to critical applications, servers and organizational governance within the cloud. Emerging businesses consuming public cloud services should make sure they follow isolated accounts for running production cloud workloads. A*	• Spoofing Identity • Tampering with Data • Repudiation • Information Disclosure • Denial of Service • Elevation of Privilege • Lateral Movement • Virtualization Threats • SaaS Web Application Specific Threats

single account to govern the billing and separate privileged accounts to run workloads should be implemented.	
Insider Attacks *These types of attacks may not be common for emerging SaaS businesses as a very small number of passionate team members are within the team. But it would definitely be a thing to worry about as the company starts to grow. So placing proper controls to manage, alert, record user activity within cloud systems, accounts are important.*	• Spoofing Identity • Tampering with Data • Information Disclosure • Elevation of Privilege • Lateral Movement • Virtualization Threats
Insecure Interfaces and APIs *Providing SaaS businesses services as APIs to customers has become a common thing. Customers often require APIs to integrate SaaS services to their systems. When exposing internal services via APIs to the outside security should be a high priority.*	• Tampering with Data • Repudiation • Information Disclosure • Elevation of Privilege • SaaS Web Application Specific Threats
Weak Control Plane *The person in charge of the cloud infrastructure should be in full*	• Tampering with Data • Information Disclosure • Elevation of Privilege • Lateral Movement

control of the data infrastructure logic flow, security and verification. Not knowing these will lead to a weak control plane.	
Metastructure and Applistructure Failures *Failing to apply proper API implementations without knowing the extent or levels that API methods should be exposed can allow unauthorized parties to access sensitive information. Also applications implemented in cloud should be able to utilize cloud to maximum effort.*	• Spoofing Identity • Tampering with Data • Repudiation • Information Disclosure • Denial of Service • Elevation of Privilege • Lateral Movement • Virtualization Threats • SaaS Web Application Specific Threats
Limited Cloud Usage Visibility *This occurs when the organization is unable to view whether the use of cloud services within the organization is malicious or not. Gartner predicts one-third of all successful security attacks would occur through this* [3]. *This won't be an issue for emerging SaaS business organizations initially. But proper controls should be placed when the company starts to grow.*	• Spoofing Identity • Tampering with Data • Repudiation • Information Disclosure • Denial of Service • Elevation of Privilege • Virtualization Threats
Abuse and Nefarious Use of Cloud Services	• Spoofing Identity • Tampering with Data

Occurs when malicious attackers use cloud resources owned by the cloud service provider itself to host malicious content. To tackle this proper incident response framework should be in place. An emerging SaaS business should make sure proper security controls are in place to make their cloud services not abused.	• Repudiation • Information Disclosure • Denial of Service • Elevation of Privilege • Lateral Movement

3.3 – Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services

Based on the details elaborated in section 2.6 in the literature review, we can see the limitations in existing cloud security models and the lack of a model to align with cloud compliance standards. Based on my research, none of the models were designed specialized focusing on emerging SaaS Cloud Systems which are entirely relying on public cloud services. The proposed model tries to solve the limitations identified and present an enhanced cloud security and compliance reference model for emerging SaaS cloud systems consuming public cloud services.

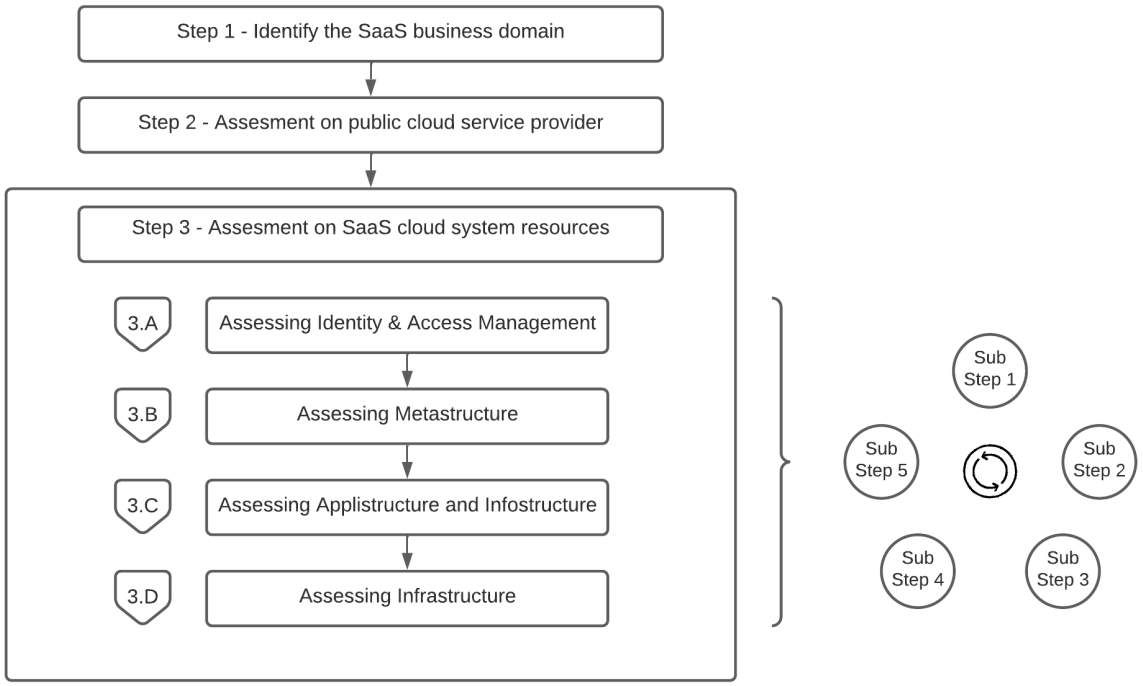
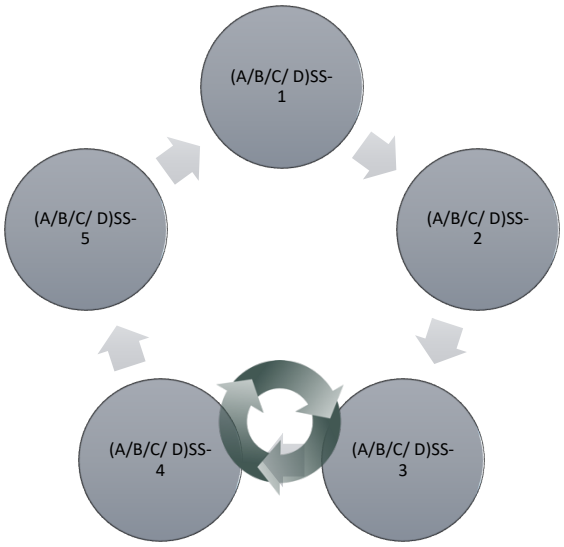


Figure 3 – Proposed Reference Model



Sub Step 1 *– Asset/ Component Identification.*

Sub Step 2 *– Assess Current Security Posture for identified elements.*

Sub Step 3 *– Identification of Cloud Threats with STRIDE-LM+*

Sub Step 4 *– Solve Identified Issues.*

Sub Step 5 *– Assess and Update the Compliance Standard posture of the SaaS Cloud System.*

Figure 4 – Assessment on SaaS Cloud System - Sub Process

3.4 – Major Components of the Proposed Model

The model proposed above consists of two main components. Figure 3 depicts the enhanced referenced model for assessing and implementing cloud security and compliance in emerging SaaS cloud systems. The assessment within SaaS Cloud System is under Step 3. It consists of four significant steps – Assessing Identity Management, Assessing Metastructure, Assessing Applistrucutre and Infostructure and Assessing Infrastructure. In each of those steps, an emerging SaaS business should go through 5 sub-steps (Figure 4). SaaS systems are expected to go through each category under Step 3 (3.A, 3.B, 3.C, 3.D) and five sub-steps under each category in Step 3 at least on an annual basis to make sure that the cloud threat level and compliance goals are at a satisfactory level. This continuous process will ensure that the identified issues using this model won't be obsolete while giving the ability to identify specific cloud threats and assess and update the SaaS cloud system compliance standards as a continuous process.

3.4.1 – Step 1 - Identify SaaS Business Domain

The main intention behind this step is to allow SaaS business management and engineering teams to understand the business domain that they are providing the services. This will enable an emerging SaaS business to identify its customers and their geographical locations. As elaborated in the literature review section 2.4, most regulatory compliance standards are based on geographical areas. So, by going through this step, emerging SaaS cloud service providers can get a clear idea of which cloud regulatory compliance standards they should focus on.

3.4.2 – Step 2 – Assessment on Public Cloud Service Provider

Since this model is intended for SaaS cloud providers consuming services of a public cloud service provider, the SaaS service provider needs to play the role of a cloud consumer in this step. As mentioned in section 2.6, the responsibility of the cloud consumer is to create a matrix to document who is implementing which controls and how are those implemented. Those should also be aligned with the compliance standards identified in Step 1. The following points need to be considered when assessing a public cloud service platform,

- Industry recognition of the selected Public Cloud Service provider.
- How secure is it? – How physical infrastructure is protected, and are security controls placed according to global standards?
- Is it audited periodically? – Get access to the audit reports; in case the SaaS business itself is audited, they should provide these documents as infrastructure like storage, network etc., is managed by the public cloud service provider.
- Is it compliant with identified regulatory compliance standard regulations? If so, find documents proving it.

3.4.3 – Step 3 – Assessment on SaaS Cloud System Resources

This step focuses on assessing cloud security and compliance in the SaaS cloud system. This consists of four major categories; in each of those categories, the 5 step sub-process needs to be applied to identify cloud threats and the status of the compliance regulation standards. STRIDE-LM+ approach can be used to determine cloud threats within the 5 step subprocess. The compliance framework features identified in step 1 can be used to assess the status of regulatory compliance standards in Step 5 of the subprocess. If the existing cloud threats or compliance levels don't align, those can be worked out in the next iteration.

The following section provides essential factors to note under each section of Step 3 of the proposed model.

Category 3. A – Assessing Identity and Access Management

This step will provide an emerging SaaS business with the ability to understand and put proper controls to manage and monitor identity and access to the cloud system resources.

Below are some critical points that emerging SaaS businesses should focus on within this step.

- Identification of users.
- Identification of user groups
- Defining user access control lists
- Defining user levels

- Create IAM policies

Category 3. B – Assessing Metastructure

The Metastructure of the cloud system focuses on the protocols and mechanisms that provide the interface between the infrastructure layer and the other layers. It's the component that ties the cloud provider technologies and enables management and configuration [21]. Since managing infrastructure is primarily a responsibility of the public cloud provider, assessing the security and compliance of the metastructure of the SaaS Cloud System is a responsibility of the SaaS business. This step will also provide emerging SaaS businesses with a complete idea of the cloud control plane of the SaaS Cloud System.

Given below are some critical points that emerging SaaS businesses should focus on within this step,

- Implement the Metastructure of the SaaS Cloud System in Infrastructure as Code.
- Implement proper security standardized configurations when setting up interfaces.

Category 3.C – Assessing Infostructure and Applistrucutre

The main focus of this step is to assess and identify the compliance and security of the infostrucutre layer and the applistructure layer of the SaaS Cloud system. The infostrucutre layer defines the data and information the SaaS cloud system holds. The Applistrucutre layer defines the applications deployed in the cloud and the underlying application services used to build them [21]. Given below are some critical points that emerging SaaS businesses should focus on within this step,

- Following Secure Coding Practices
- Make sure data and information security are a top priority.
- Application vulnerability analysis intrusion detection mechanisms should be built.
- Use data encryption methods for data in rest as well as in transit.
- Create good data retention log collection policies aligning with the regulatory compliance standards.

Category 3.D – Assessing Infrastructure

The primary focus of this step is to assess and identify the compliance and security of the infrastructure layer of the SaaS cloud system. This step shouldn't be confused with step 2 of assessing the public cloud service provider as most of the infrastructure controls will be managed by the cloud service provider. But as discussed earlier, based on the shared responsibility model, the SaaS service provider is expected to focus on the responsibility associated with the infrastructure layer as the cloud consumer in this layer. Given below are some critical points that emerging SaaS businesses should focus on within this step,

- Usage of securely hardened and verified golden OS images.
- Focus on only providing the OS images with required ports, protocols, and services to meet business needs using technical controls.
- Implementation of IDS/ IPS tools to facilitate timely detection and identification of root causes of internal security incidents.
- Ability to restrict access to all cloud administrative consoles based on minor privilege principles and supported through technical controls such as two-factor authentications, IP based filtering etc.
- Ability to patch vulnerabilities across all the cloud computing devices, applications and systems.
- Secure cloud infrastructure and applications using anti-virus programs.

3.5 – Mapping between the proposed reference model and CSA CCM (Cloud Control Matrix) domains

THE IMPORTANCE OF the CSA CCM domains were initially discussed in section 2.3 of the literature review. The CSA CCM v3.0.1 publication and domains could be identified as the most updated and only security controls created specifically targeting cloud delivery models. Also, the availability of mappings between CSA CCM to major regulatory/ compliance standards and security frameworks worldwide makes any model mapped into CSA CCM easily mapped with those popular standards and frameworks.

3.5.1 – Selection of the most critical cloud controls from the CSA CCM domains depending on the identifications of the latest top cloud threats publication

The main reason behind this step was to identify the most critical CSA CCM domains that emerging SaaS businesses should focus on. It was decided based on the CSA's top cloud threats publication [3]. The CSA CCM v3.0.1 consists of 16 cloud control domains. Out of those, only 13 cloud control domains have been identified as directly related to the latest top cloud threats [3]. This was also validated within [49], a deep dive study into real-world cloud threat-related cases study. Based on that study, mitigations and controls associated with 9 case studies cover 13 of 16 CSA control domains. The primary reason for this was that the Data Center Services (CDS) control principally covers data center operations done by cloud service provider facilities. The Mobile Security (MOS) control includes safeguards typically utilized in enterprise environments. This statement further strengthens the decision to remove the CDS and MOS controls from the mapping between CSA CCM domains and the proposed reference model as our primary focus here is emerging SaaS businesses utilizing public cloud services. Though the above study didn't identify any cloud threats linked to the Interoperability & Portability (IPY) control, it was selected for mapping with the proposed reference model as it covers controls associated with Application Programming Interfaces (APIs). According to many studies, this inclusion can be validated as the APIs are considered the next big SaaS wave [47]. Hence, SaaS businesses must ensure the security and compliance standards of the APIs that they expose externally. With further inspection of these controls, a decision was made to omit the Supply Chain Management, Transparency & Accountability (STA) control as it was mainly covered within step 2 of the proposed reference model (Step 2 - Assessment on Public Cloud Service Provider).

A complete mapping between the latest top most cloud threats published within [3] and the CSA Cloud control domains can be found in Appendix A.

The 13 controls that were finalized for the mapping are,

1. Application and Interface Security (AIS)
2. Audit Assurance and Compliance (AAC)
3. Business Continuity Mgmt. & Operational Resilience (BCR)

4. Change Control & Configuration Management (CCC)
5. Data Security & Information Lifecycle Management (DSI)
6. Encryption & Key Management (EKM)
7. Governance & Risk Management (GRM)
8. Human Resources Security (HRS)
9. Identity & Access Management (IAM)
10. Infrastructure & Virtualization Security (IVS)
11. Security Incident Management, E-Disc & Cloud Forensics (SEF)
12. Interoperability & Portability (IPY)
13. Threat & Vulnerability Management (TVM)

3.5.2 – Mapping of CSA CCM domains with the proposed reference model

The direct mapping has been carried out with the categories under Step 3 – Assessing SaaS cloud system resources since it's the most significant step within the proposed model that captures SaaS cloud systems' compliance and security requirements.

3.5.2.1 – CSA CCM domains associated with Category 3.A – Assessing Identity & Access Management

The Identity & Access Management (IAM) domain was directly mapped into category 3.A. It covers all security and compliance controls related to SaaS system identity and access management.

3.5.2.2 – CSA CCM domains associated with Category 3.B – Assessing Metastructure

As discussed in section 3.B, the metastructure of the SaaS cloud system is the component that ties the cloud provider technologies and enables management and configuration [21]. Hence CCM controls associated with managing and configuring the cloud provider technologies were mapped to this category. Those controls are,

- AAC
- CCC

- SEF
- BCR
- GRM
- HRS
- EKM

3.5.2.3 – CSA CCM domains associated with Category 3.C – Assessing Applistructure and Infostructure

As discussed in section 3.C, the infostrucutre layer defines the data and information the SaaS cloud system holds. The applistructure layer defines the applications deployed in the cloud and the underlying application services used to build them [21]. Hence, CCM controls focusing on the applistructure, and infostructure layers were mapped into this category. Those controls are,

- AIS
- IPY
- DSI

3.5.2.4 – CSA CCM domains associated with Category 3.D – Assessing Infrastructure

As discussed in section 3.D, the infrastructure mentioned within this section focuses on the SaaS service providers' responsibility to ensure that the infrastructure services used within the public cloud service provider are appropriately managed based on security best practices. Based on that, the CCM controls focus on the infrastructure services were mapped into this category. Those controls are,

- IVS
- TVM

Table 6 – Mapping between categories within the assessing SaaS cloud system resources step of the proposed reference model with CSA CCM domains.

Assessing Identity and Access Management (3.A)	IAM						
Assessing Metastructure (3.B)	AAC	CCC	SEF	BCR	GRM	HRS	EKM
Assessing Applistructure and Infrastructure (3.C)	AIS	IPY	DSI				
Assessing Infrastructure (3.D)	IVS	TVM					

3.6 – Conclusive Remarks

The Methodology chapter highlights improvements and solutions to existing limitations identified within the Literature Review chapter. This chapter proposes a new threat modelling approach specifically designed to assess threats related to SaaS cloud systems. Each of those solutions and improvements were taken into account when creating the enhanced cloud security and compliance reference model for emerging SaaS cloud systems consuming public cloud services. The final part of the chapter focuses on presenting the enhanced reference model and mapping it with existing CSA CCM cloud control domains which were filtered based on top cloud threats.

4 – IMPLEMENTATION

This section discusses a detailed overview of the implementation phase carried out within this research. As discussed within the research objectives, the motive behind this implementation was to show how the proposed reference model could be used more practically and effectively in the real world. There was a massive challenge in identifying what would necessarily be the implementation that would allow achieving the motive discussed earlier. For such a model to be effective and practical, there should also be ways to easily be consumed by emerging SaaS businesses to assess their cloud security and compliance status.

As identified within the Introduction chapter and a part of the research problem that we are trying to solve, the emerging SaaS businesses have limitations regarding having enough resources to assess their security and compliance status. Even though I have proposed a detailed reference model for evaluating SaaS cloud system resource security and compliance status, it won't be successful if the SaaS business doesn't know what factors to assess within each category. So, the implementation phase was carried out to determine those factors. Based on the literature review, I have identified that the best way to achieve this was by creating a set of audit questions for each of the categories identified within the proposed reference model.

But by, simply answering a set of audit questions on cloud security and compliance without knowing what it means or without any insight will be pointless for an emerging SaaS business. It will become another reference model that requires manual effort and domain knowledge to assess your SaaS system's cloud security and compliance level. The implementation should also include a feedback mechanism where it can provide its users with some additional insights and recommendations on what to do with their current level of security and compliance in their SaaS system. The current security and compliance status under each category of the proposed model can be assessed by the audit question responses per category. Then this could be extended into providing insights and recommendations to the user based on the proposed reference model. But the insights and recommendation prediction part based on audit question responses should be future-proof and adaptive. This could be achieved by incorporating machine learning techniques to identify different user responses to audit questions rather than manual categorizing. Hence a significant focus of this implementation was given to designing and developing of machine learning models to achieve what we have discussed above.

Another critical part of this implementation was to create a way to allow users to interact with the proposed reference model and the machine learning model built on top of it. As more and more engineering teams are looking into ways of automating manual jobs and programmatically accessing different systems exposed via APIs, the decision was taken to expose this implementation as an API service. This will allow any party trying to use the proposed reference model to interact with it programmatically, understand their current security and compliance status, and obtain insights on what should be the next step in improving that status or maintaining it. This will also allow the proposed reference model to be widely and easily adopted while allowing a universal way for users to interact with the model. This can be identified as the first of its kind compared to a cloud security and compliance reference model designed before this research attempt.

To further strengthen the ability to consume the proposed reference model in the real world, a mapping of NIST 800-53 Revision 5 control domains with the proposed reference model was also implemented and presented in the final section of this chapter (Section 4.3). This allows users to map the compliance status of the proposed reference model to many other regulatory compliance standards, including GDPR, CCPA and ISO/IEC 27001 etc.

4.1 – Implementation of the machine learning model

4.1.1 – Data collection and organization

Machine learning consists of three main components. These can be identified as data, features and algorithms [50]. Data can be identified as the most critical part of a machine learning model. The success rate of the machine learning model is directly proportional to the quality of the data collected. So, the data collection part is the most critical step in building a machine learning model.

As we have discussed in detail within section 2.7 under Literature Review, the best way to generate a training data set which is accurate for the machine learning model that we are trying to implement was based on a survey questionnaire. The idea behind the survey questionnaire was to capture respondents' answers and whether they are compliant with security and compliance controls that are expected within the proposed reference model. This type of data

collection technique is often identified as crowdsourcing. The question set for the survey was based on a questionnaire that is already used within the real world to gauge a cloud system's security and compliance levels.

A key research objective was to map the proposed reference model with the industry's existing and widely adopted regulatory/compliance standards and security reference models. I have created a mapping between the CSA CCM controls and the proposed reference model, discussed in detail within the Methodology section. The exact mapping which was introduced in section 3.5 within the Methodology chapter was used to categorize the survey questions with the proposed reference model.

The creation of a question set for the final survey used for data collection had to be carried out in multiple attempts. The main reason for that was the challenges faced while designing the study. In the initial effort, the CSA Assessment Initiative Questionnaire (CAIQ) v3.0.1 [51] was referred to identify audit questions which are directly mapped to each control within the CSA CCM. Based on the mapping created between the CSA CCM and the categories within the core step of the proposed reference model, a direct correlation between the CAIQ questions and the categories identified within the proposed reference model was created.

But the total number of questions identified were close to 150. Based on further refining and removing the CSA CCM controls that are not mapped to the proposed reference model and explicitly focusing on the SaaS domain, I reduced the question number to 110. But as the survey was created with these 110 questions and shared with a selected group of respondents to assess the clarity of the survey, it was identified that they were taking more than 20 minutes to complete the survey with its large question set. So, a further filtration of questions was required as going forward with the same approach would directly affect the survey completion rate and bring down the responses for the training data set. Within the next attempt, I was able to identify a more concise version of the CAIQ v3.0.1 (CAIQ-Lite) published by a collaborative effort between CSA and Whistic [47]. Compared to the original CAIQ version, the CAIQ-Lite consisted of around 73 questions. So based on my mapping of the proposed reference model with the CSA CCM controls and SaaS domain-specific filtrations, I was able to drill down further into the CAIQ-Lite questionnaire, which included 53 questions in total. This can be considered a significant improvement compared to the previous attempts as it almost doubled

the response rate and reduced the time of completion of the final survey. The same set of survey respondents' who filled the survey created within the initial attempt said that the clarity of the survey was improved. The final survey question set can be accessed in Appendix B and C.

Figure 5 shows the step-by-step process of creating a correlation between the proposed reference model, the CSA CCM domains and the question set under each domain. Steps 1 and 2 of this process were discussed in section 3.5.1 within the Methodology chapter in detail.

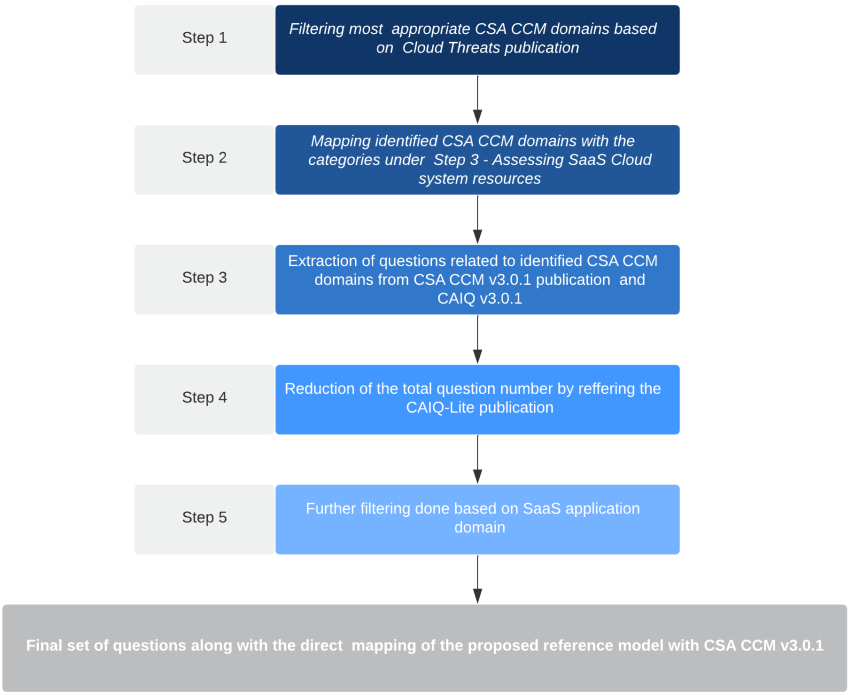


Figure 5 – Step-by-step process involved in the creation of correlation between the CSA CCM domains and the question set under each domain

The survey was shared among the Sri Lankan IT community who mainly worked or had previous experience working with cloud-based systems. All the survey findings are presented within the Analysis and Findings chapter.

The survey consisted of four sections, focusing on a major component or a step within the proposed reference model. Those four significant sections and their focus areas can be listed as follows,

1) Intro Questionnaire

- Identification of SaaS business type.
- Identification of survey respondent's profile.

2) Assessing SaaS business domain
    - Identification of the business domain of the SaaS platform
    - Identification of the geographical locations and the regulatory compliance standard awareness of the SaaS business.
3) Assessing the Cloud Service Provider
    - Identification of the knowledge of the SaaS business around the shared responsibility model.
    - Identification of CSP products used by the respondents of the survey.
4) Assessing SaaS Cloud system resources
    - Assessing Identity Management and Access
    - Assessing Metastructure
    - Assessing Applistructure and Infostructure
    - Assessing Infrastructure

After the survey was shared, a total of 51 responses were received.

The CSA CCM controls were mapped with the Step 3 - Assessing SaaS Cloud System Resources section of the proposed reference model as it's the core component within the proposed reference model. Hence the machine learning model was designed by only taking responses and questions from section 4 of the survey into account. Appendix C consists of a mapping between the survey questions under Assessing SaaS Cloud system resources to each subcategory within Step 3 of the proposed reference model. It also includes the CSA CCM control domain to which each question belongs. Each question was assigned with a unique id to detect those easily.

All questions were audit-type questions and expected answers like Yes/No or N/A (not applicable). Based on my research, I identified that for a SaaS startup to be compliant and secure, they have to respond Yes to most of these questions. In contrast, some questions can be answered as No or N/A depending on the applicability of that question. Identification of details within the survey question set was crucial as its very important for these details to be converted as insights to the user within the final implementation. Table 7 presents the

mandatory question ids that belong to each subcategory under Step 3 of the proposed reference model. Refer Appendix C to obtain questions denoted by the given ids.

Table 7 – Mapping between subcategories under Assessing SaaS cloud resources with individual question ids

Step 3 – Subcategory title of the proposed reference model	Mandatory Question IDs (Refer Appendix C for questions denoted by Ids)
Assessing Identity and Access Management (3.A)	A1, A2, A3, A4, A5, A8, A9
Assessing Metastructure (3.B)	B3, B2, B4, B5, B6, B7, B9, B10, B11, B12, B13, B14, B15, B16, B17, B19, B20, B21, B22, B23, B24, B25
Assessing Applistructure and Infostructure (3.C)	C1, C2, C3, C4, C6, C7, C8, C9, C10
Assessing Infrastructure (3.D)	D1, D2, D3, D4, D6, D7, D8, D9

4.1.2 – Feature selection for the machine learning model

As discussed earlier, feature selection is a vital part of a machine learning process and directly impacts how well the machine learning model can be trained. So, selecting and optimizing the data set's features was vital to how well a model can be trained on the data. These can be identified as variables or parameters. The specified features will be the factors that the machine learning model will look at and make predictions by learning the values derived for those features.

The final data set had responses for questions under four primary categories - 3.A, 3.B, 3.C, and 3.D. Based on the implementation design, the main requirement was to identify a way to provide status and insights on the SaaS system’s resources. This can only be predicted by identifying the responses given to each question. So, it was clear that each question under each category had to be taken as a feature of the machine learning model. Yet again, the number of questions was high (53), which meant that we had to analyze 53 features within the machine learning model, which was a very high number for a feature set. As our training data set was

around 51 records, going ahead with that number of features had a clear impact on reducing the quality of the machine learning model.

Since my domain knowledge in this area was very limited, I had to reach out to an expert within the machine learning domain and identify the best approach in the feature selection process. In a personal interview, Rashmika Nawaratne explained the importance of reducing the number of features within a machine learning model, which validated my previous assumptions. Also, the idea of developing multiple machine learning models per category were identified as the best approach to reduce the number of features that each machine learning model had to analyze. By further analyzing the data set, it was determined that questions within each category could be further divided into two categories as cloud governance and operations based on how the cloud resources are controlled and managed. This further increased the number of categories, and as a result, the number of features per category was reduced.

The feature selection process helped us understand the training data set and the details required to implement the machine learning model. The understanding led to creating eight different machine learning models per category independent of each other for the final implementation.

Figure 6 presents the components breakdown flow within the feature categorization process.

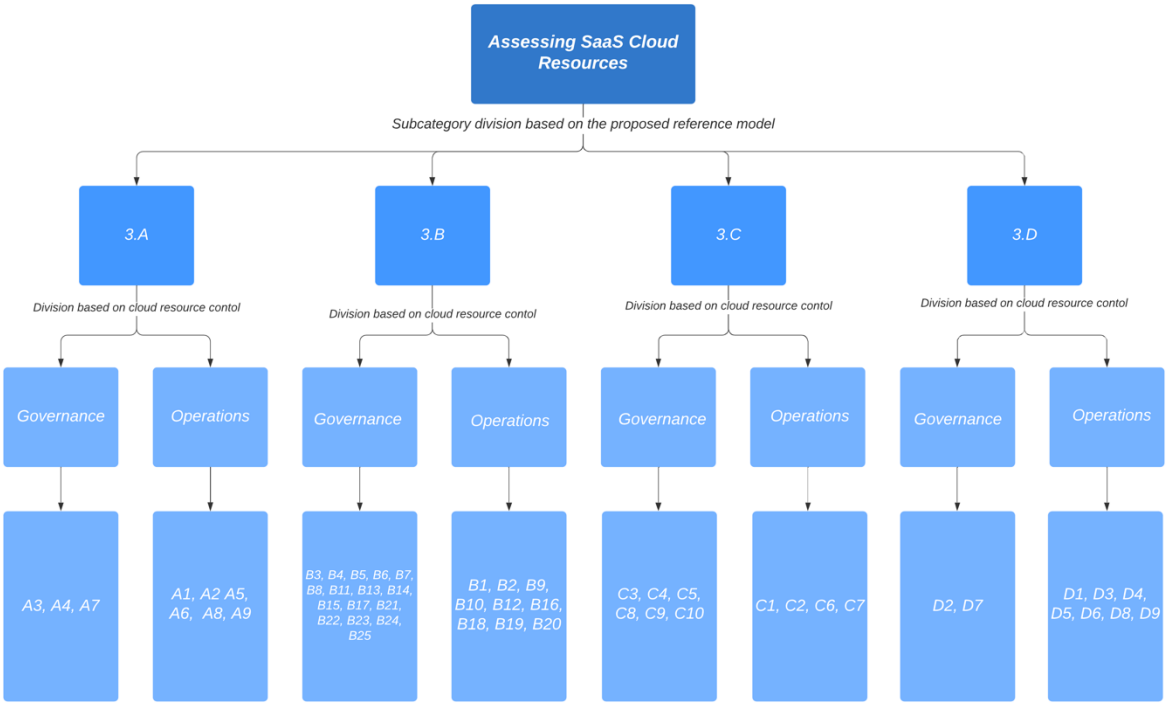


Figure 6 – Component breakdown flow in the feature categorization process

4.1.3 – Selection of machine learning type and the algorithm

Machine learning tasks can be mainly classified into two main learning types. Those are supervised learning and unsupervised learning. In supervised learning, the labelled data is used to train the model. These labels for the training data set represent the category each data observation belongs to. After introducing a supervised learning model, the model should predict the label that new data observations belong to [51]. The unsupervised learning type uses unlabeled data, which allows the model to learn new relationships and pick up underlying patterns from the data observations [52]. All unsupervised learning algorithms are based on finding the similarities/ differences between data observations and making conclusions based on those findings [53].

As we examine our data set and the feature selection process, it's clear that identifying labels within that data set will not work as all the features within the data set can be considered unlabeled. Hence applying the supervised learning type was not ideal. With an unlabeled data set, it's clear that unsupervised learning was the ideal machine learning type for this implementation.

The most commonly used type of unsupervised learning is clustering [53]. As the name suggests, clustering algorithms will cluster data into distinct groups. As defined within the research objectives and several other places within this thesis, the main focus of the implementation was to provide insights and recommendations on the security and compliance status of a SaaS system. To achieve this, we should identify different types of clusters or groups for each data observation within the training data set. By doing that, we get the ability to interpret those clusters. So, when new data observations are passed to the implemented machine learning model, those data will be assigned to a pre-interpreted cluster based on the similarities/ differences, which was done in the machine learning model development/ training step. We can provide a pre-defined set of insights and recommendations on the security and compliance status of the SaaS system based on the cluster to which the new data observation belongs.

The selection of a clustering algorithm that was ideal for this implementation was made after doing a literature review on existing research in this area and many other available resources.

This attempt was discussed in detail within section 2.7 in the Literature Review chapter. The K-Mode clustering algorithm with Cao initialization was selected as the algorithm used for the machine learning model implementation. The K-Modes algorithm was chosen as the data set, and features consist of categorical variables compared to numerical ones. The Cao initialization type for the K-Modes was used as it was identified to be performing better compared to Huang initialization [48].

4.1.4 – Data Preprocessing

This step was carried out to ensure that the collected data set is processed in a usable format for the training of the machine learning model. This consisted of two parts where processing was carried out manually and programmatically.

In the manual step, all the data collected from the survey had to be categorized and divided based on the categorization process carried out in the feature selection step. After that, each data per category was stored in separate CSV files. Each column represented the set of features under each category, and rows represented the data observation for each feature. The final data sets created per category are available within Appendices D to K.

The programmatical phase focused on the data pre-processing within the data observations under each data set categorized in the manual step. Steps have been carried out to ensure that those data sets didn't include any missing data. Also, the label encoding process has been carried out to change the categorical data, which is text-based, to numbers as machines can only understand numbers.

4.1.5 – Selection of technologies/ tools

The focus of this step was to identify which technologies and tools to use to implement the machine learning model.

The initial focus was on selecting the programming language to develop the machine learning model. Python was chosen without hesitation as it is considered the most popular and widely adopted programming language used to build machine learning models. The primary reason

behind it was that it included excellent community support, commonly adopted in the industry for machine learning tasks, and most importantly plethora of libraries available to carry out data pre-processing/ manipulations and machine learning algorithms. Jupiter Notebook was selected as the IDE to implement this machine learning model. It was also chosen based on its wide popularity within the machine learning community as an IDE for machine learning tasks.

Table 8 lists the libraries that were used to perform specific tasks within the machine learning model development phase.

Table 8 – Python libraries used and their use cases

Library	**Use case**
numpy	For data manipulations
pandas	For data analysis
matplotlib.pyplot	For graphs and charts plotting
sklearn	For data pre-processing
kmodes.kmodes	KModes clustering algorithm implementation

4.1.6 – Final Implementation

4.1.6.1 – Machine learning model code analysis

This section provides a walk-through of the machine learning model implementation code. The data pre-processing steps and the model training methodology were similar in all the models built per category. The only changes were the data source and the clusters derived after the trained model.

The code related to each section within the machine learning model implementation is covered below.

Import the required data manipulation, analysis, processing, and visualization libraries

```
# Importing required libraries
import numpy as np
import pandas as pd
from kmodes.kmodes import KModes
from sklearn import preprocessing

# Data vizualization libs
import matplotlib.pyplot as plt
import seaborn as sns
%matplotlib inline
```

Figure 7 – ML code analysis - Import the required libraries

Source data from training data set CSV file as a data frame for data manipulation

```
df = pd.read_csv("/Users/ravindufernando/Documents/MSc Content/MSc Project/ml-analysis/datasets/gov_ops_clusters/cat_
df.head()
```

Figure 8 – ML code analysis – Reading and conversion of the training data set

Identify the dimensions and inspection of the training data set data frame

```
cat_a_gov_for_kmodes = df.copy()

cat_a_gov_for_kmodes.shape
cat_a_gov_for_kmodes.describe()
cat_a_gov_for_kmodes.info()
```

```
cat_a_gov_for_kmodes.isnull().sum()*100/cat_a_gov_for_kmodes.shape[0] # Checking for null values
```

Figure 9 – ML code analysis – Training Data set inspection

Data pre-processing step of removing null values and replacing with default values and label encoding to encode text values to integer values

```
# Custom Label Encoding
cat_a_gov_for_kmodes.replace(np.nan, 'notapplicable', inplace=True)
#cat_a_gov_for_kmodes.replace(('Yes', 'No'), ('2', '1'), inplace=True)

le = preprocessing.LabelEncoder()
cat_a_gov_for_kmodes = cat_a_gov_for_kmodes.apply(le.fit_transform)
```

Figure 10 – ML code analysis – Data Pre-processing

Calculation of cost (sum of all dissimilarities between clusters) using the cost function for a range of k values

```
cost = []
for num_clusters in list(range(1,10)):
    kmode = KModes(n_clusters=num_clusters, init = "Cao", n_init = 1, verbose=1)
    kmode.fit_predict(cat_a_gov_for_kmodes)
    cost.append(kmode.cost_)
```

Figure 11 – ML code analysis – Calculation of cost for a range of k values

Plotting the cost function to k (clusters) graph to visually identify optimal value for k (clusters) using elbow method

```
y = np.array([i for i in range(1,10,1)])
plt.plot(y,cost)
plt.xlabel('k clusters')
plt.ylabel('Cost')
plt.title('Elbow Method For Optimal k')
plt.show()
```

Figure 12 – ML code analysis – Plotting the cost function to a range of k values

KModes clustering on the training data set with the optimal number of k values selected as the n_clusters

```
km_cao = KModes(n_clusters=3, init = "Cao", n_init = 1, verbose=1)
fitClusters_cao = km_cao.fit_predict(cat_a_gov_for_kmodes)
```

Figure 13 – ML code analysis – KModes Clustering

Appending the identified cluster value to each data observation to analyze data validations

```
cat_a_gov_for_kmodes['Clusters'] = fitClusters_cao
```

Figure 14 – ML code analysis – Appending of cluster values to the original data frame

4.1.6.2 – Outputs of the final machine learning models implemented

This section presents the outputs of the machine learning models created per each category. Each of the implemented machine models' expected result was the optimal number of clusters that should be used for clustering on the training data set and identifying how we want to interpret those. The Elbow method was used to determine the optimal number of clusters. The principle behind it was to take the value of k (clusters) at the point when the cost value does not decrease significantly with the addition of the value of k (clusters). This was determined by visually plotting each k (cluster) cost for a range of k values. The cost is the sum of all dissimilarities between the clusters. The code related to this process is presented in section 4.2.3.

Machine learning model outputs for Category A – Governance

The graph depicted in Figure 15 shows the variation of cost for each k (clusters) for the Category A – Governance data set.

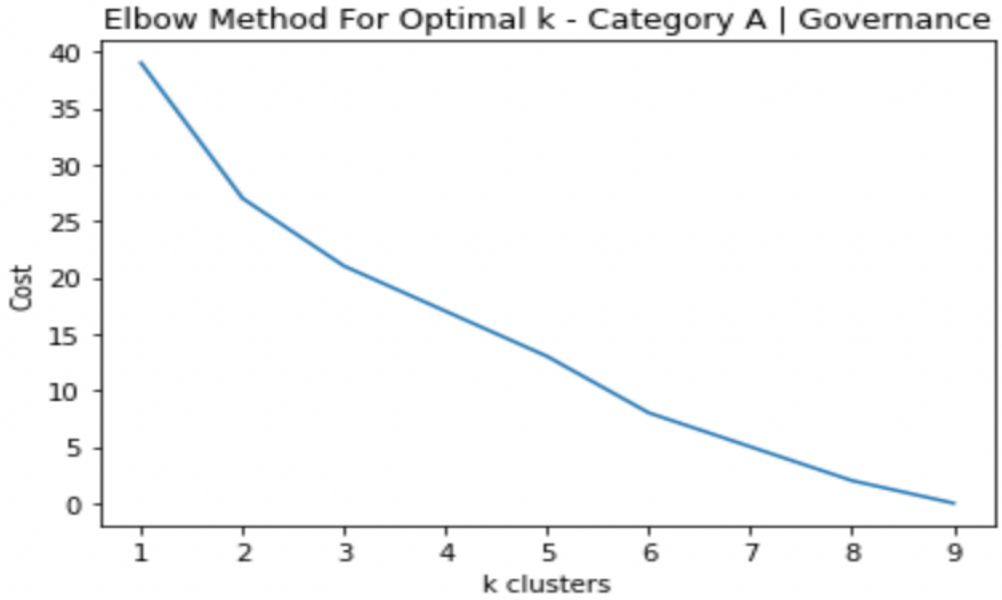


Figure 15 – Elbow method for optimal k – Category A | Governance

As the graph in Figure 15 depicts, the cost value doesn't significantly decrease after the k value of three, which means the optimal cluster value can be chosen as three for this case. The table under Appendix D shows the cluster to which each data observation belongs in the training

data set after running the KModes algorithm with three as the number of clusters. Please note that the values of the data observations are label encoded, where Yes value encoded as 1, No value encoded as 0, and Not Applicable value encoded as 2.

Machine learning model outputs for Category A - Operations

The graph depicted in Figure 16 shows the variation of cost for each k (clusters) for the Category A – Operations data set.

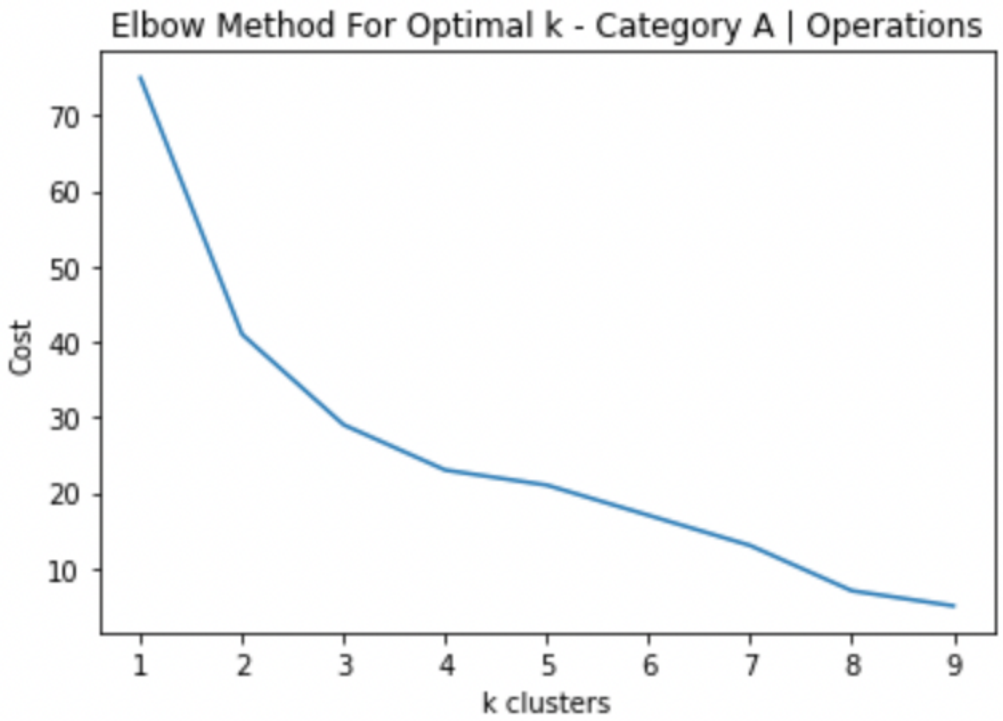


Figure 16 – Elbow method for optimal k – Category A | Operations

As the graph in Figure 16 depicts, the cost value doesn't significantly decrease after the k value of four, which means the optimal cluster value can be chosen as four for this case. The table under Appendix E shows the cluster each data observation belongs to in the training data set after running the KModes algorithm, with four as the number of clusters. Please note that the values of the data observations are label encoded, where Yes value encoded as 1, No value encoded as 0, and Not Applicable value encoded as 2.

Machine learning model outputs for Category B - Governance

The graph depicted in Figure 17 shows the variation of cost for each k (clusters) for the Category B – Governance data set.

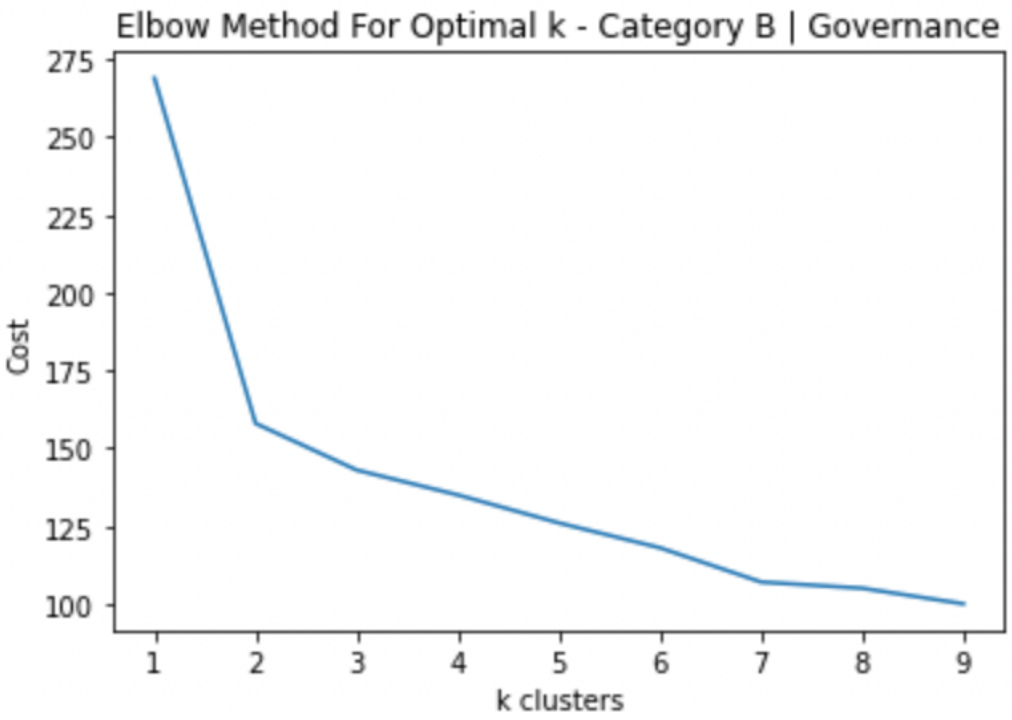


Figure 17 – Elbow method for optimal k – Category B | Governance

As the graph in Figure 17 depicts, the cost value doesn't significantly decrease after the k value of three, which means the optimal cluster value can be chosen as three for this case. The table under Appendix F shows the cluster to which each data observation belongs in the training data set after running the KModes algorithm with three as the number of clusters. Please note that the values of the data observations are label encoded, where Yes value encoded as 1, No value encoded as 0, and Not Applicable value encoded as 2.

Machine learning model outputs for Category B - Operations

The graph depicted in Figure 18 shows the variation of cost for each k (clusters) for the Category B – Operations data set.

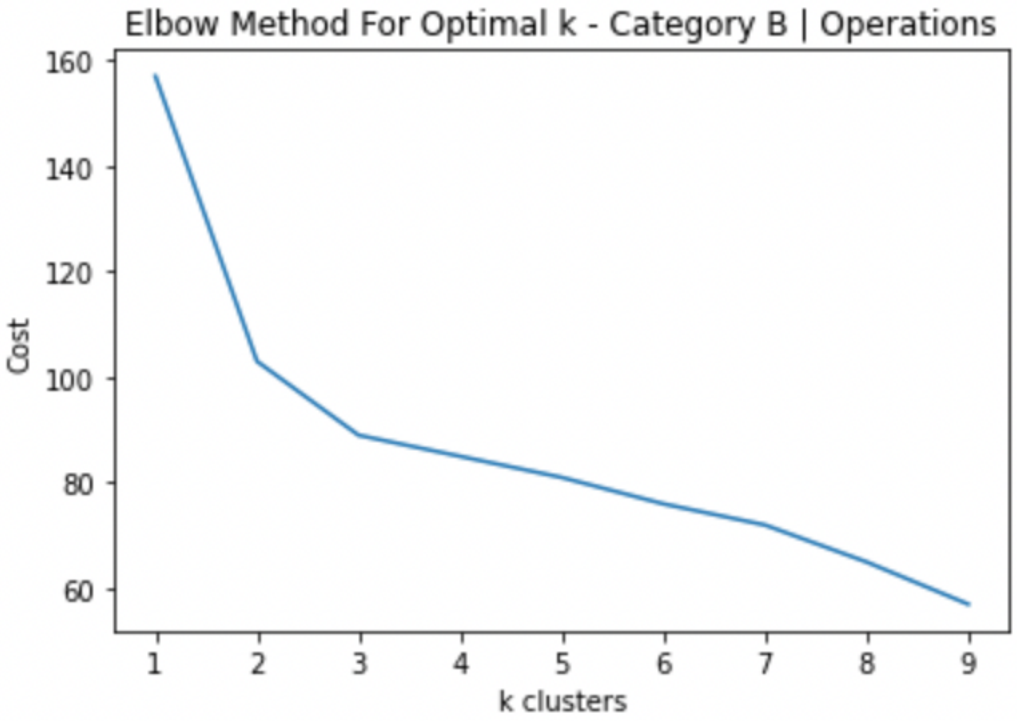


Figure 18 – Elbow method for optimal k – Category B | Operations

As the graph in Figure 18 depicts, the cost value doesn't significantly decrease after the k value of three, which means the optimal cluster value can be chosen as three for this case. The table under Appendix G shows the cluster to which each data observation belongs in the training data set after running the KModes algorithm, with three as the number of clusters. Please note that the values of the data observations are label encoded, where Yes value encoded as 1, No value encoded as 0, and Not Applicable value encoded as 2.

Machine learning model outputs for Category C - Governance

The graph depicted in Figure 19 shows the variation of cost for each k (clusters) for the Category C – Governance data set.

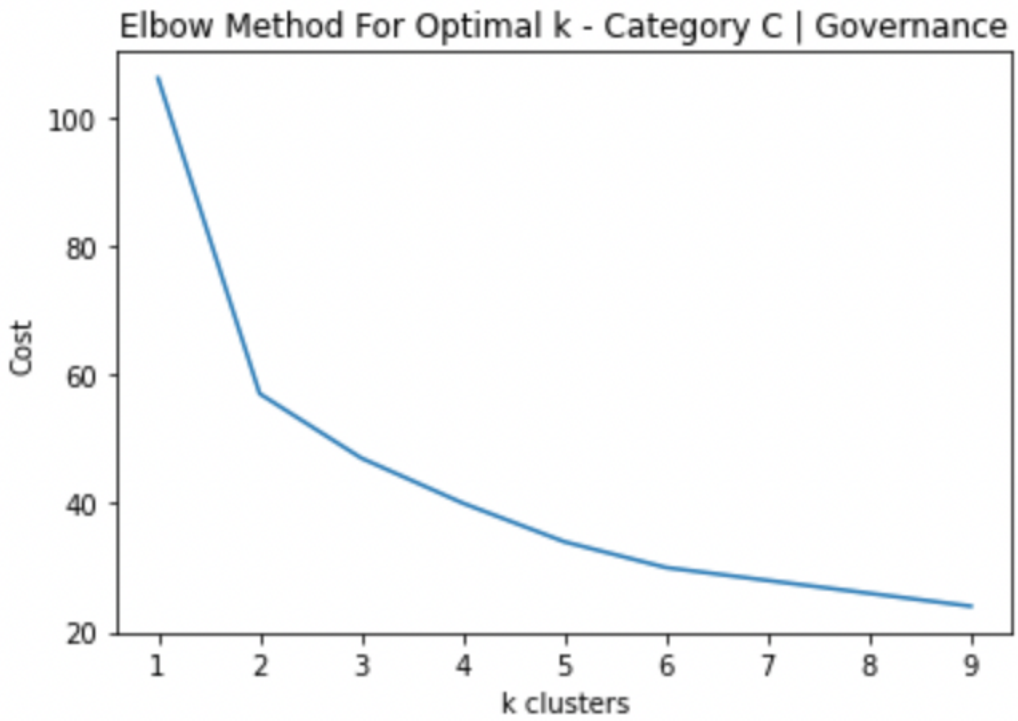


Figure 19 – Elbow method for optimal k – Category C | Governance

As the graph in Figure 19 depicts, the cost value doesn't significantly decrease after the k value of three, which means the optimal cluster value can be chosen as three for this case. The table under Appendix H shows the cluster to which each data observation belongs in the training data set after running the KModes algorithm, with three as the number of clusters. Please note that the values of the data observations are label encoded, where Yes value encoded as 1, No value encoded as 0, and Not Applicable value encoded as 2.

Machine learning model outputs for Category C - Operations

The graph depicted in Figure 20 shows the variation of cost for each k (clusters) for the Category C – Operations data set.

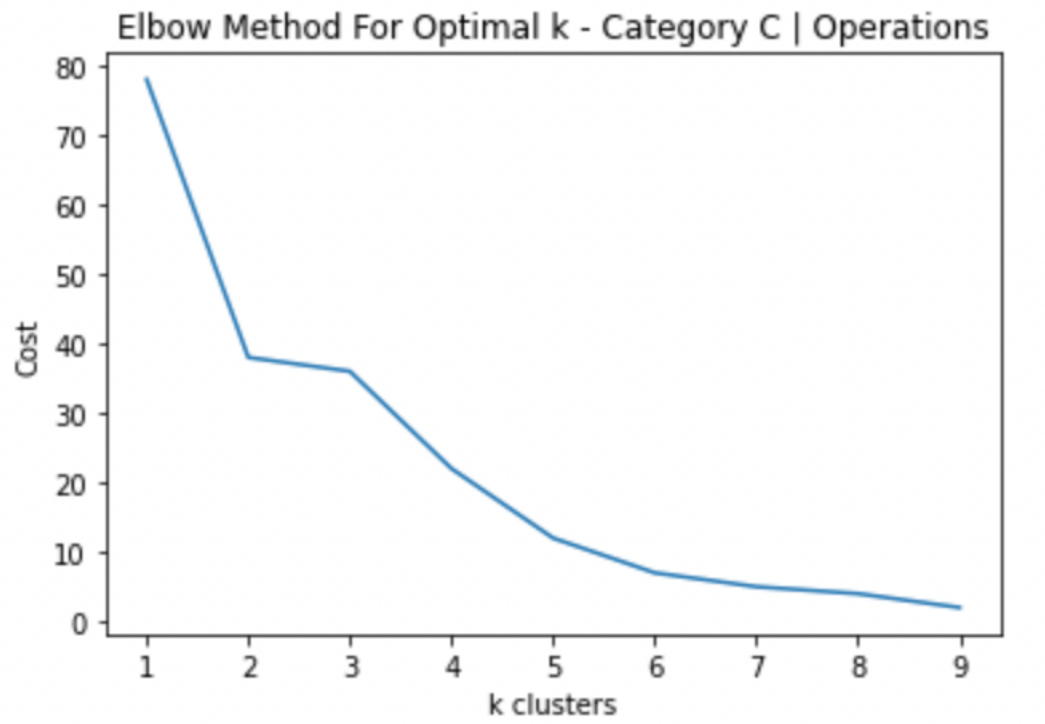


Figure 20 – Elbow method for optimal k – Category C | Operations

As the graph in Figure 20 depicts, the cost value doesn't significantly decrease after the k value of five, which means the optimal cluster value can be chosen as five for this case. Appendix I shows the cluster to which each data observation belongs in the training data set after running the KModes algorithm with five as the number of clusters. Please note that the values of the data observations are label encoded, where Yes value encoded as 1, No value encoded as 0, and Not Applicable value encoded as 2.

Machine learning model outputs for Category D - Governance

The graph depicted in Figure 21 shows the variation of cost for each k (clusters) for the Category D – Governance data set.

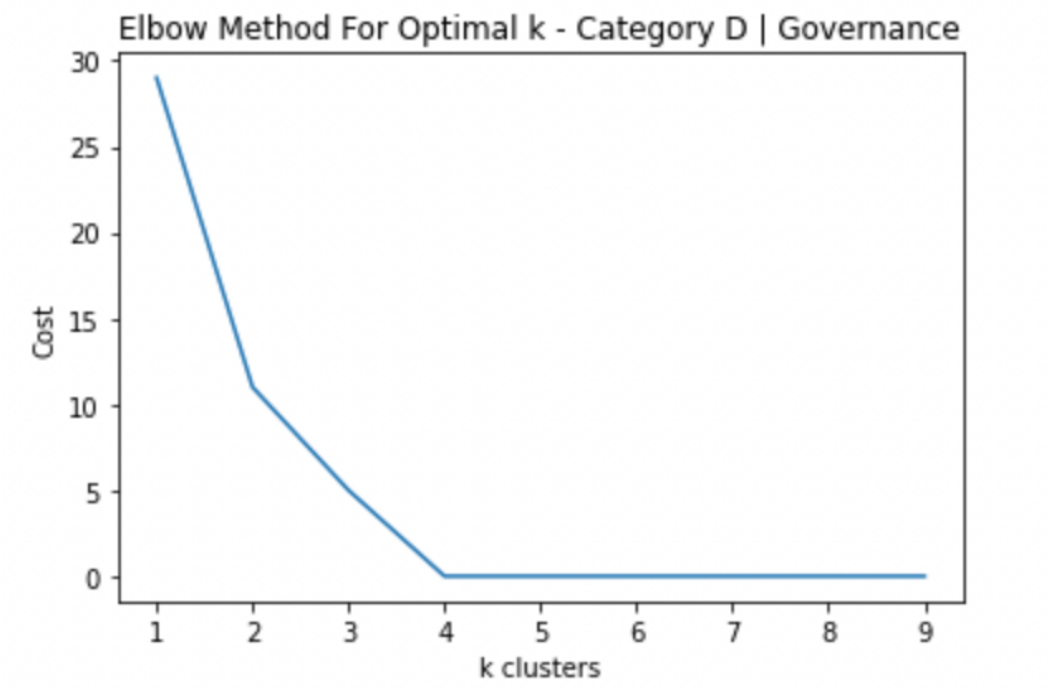


Figure 21 – Elbow method for optimal k – Category D | Governance

As the graph in Figure 21 depicts, the cost value doesn't significantly decrease after the k value of four, which means the optimal cluster value can be chosen as four for this case. The table under Appendix J shows the cluster to which each data observation belongs in the training data set after running the KModes algorithm, with four as the number of clusters. Please note that the values of the data observations are label encoded, where Yes value encoded as 1, No value encoded as 0, and Not Applicable value encoded as 2.

Machine learning model outputs for Category D - Operations

The graph depicted in Figure 22 shows the variation of cost for each k (clusters) for the Category D – Operations data set.

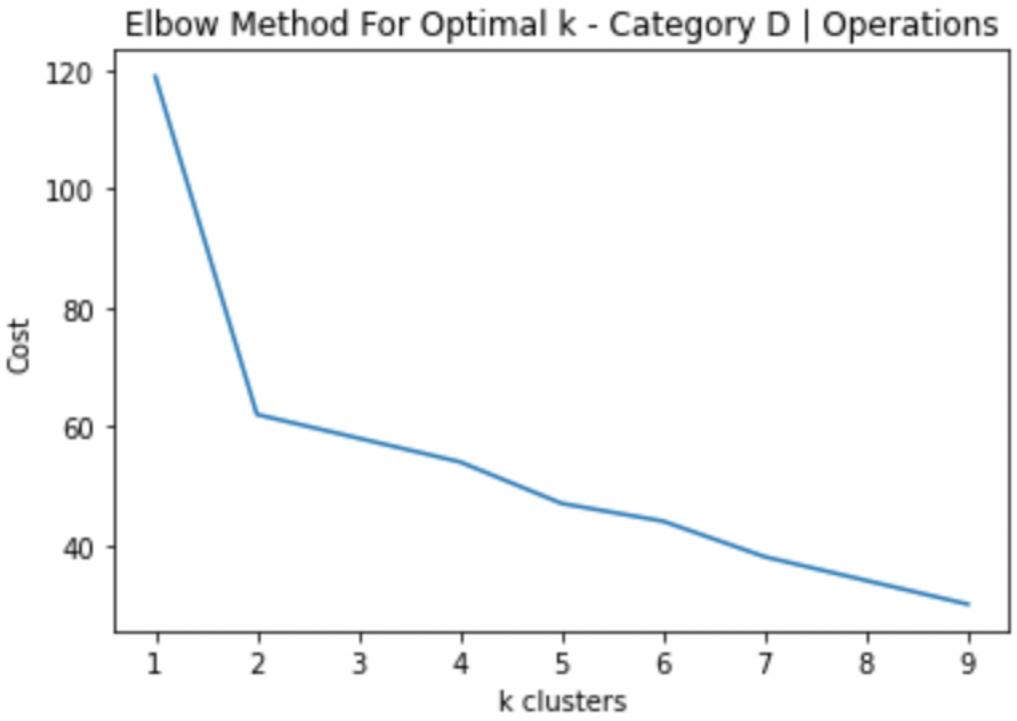


Figure 22 – Elbow method for optimal k – Category D | Operations

As the graph in Figure 22 depicts, the cost value doesn't significantly decrease after the k value of four, which means the optimal cluster value can be chosen as four for this case. The table under the Appendix K the cluster to which each data observation belongs in the training data set after running the KModes algorithm with four as the number of clusters. Please note that the values of the data observations are label encoded, where Yes value encoded as 1, No value encoded as 0, and Not Applicable value encoded as 2.

4.1.6.3 – Cluster interpretations

This section presents the interpretations created for clusters under each category. When looking at the audit questions and considering practical scenarios, there can be mainly three types of SaaS system security and compliance statuses.

- Type 1 – SaaS systems that are very secure and are compliant with almost all the audit questions.
- Type 2 – SaaS systems that aren't secure and aren't compliant with either almost or a significant percentage of audit questions.

- Type 3 – SaaS systems that are secure but has room to improve. They are compliant with the majority of the audit questions but partially.

Cluster interpretation was carried out, taking the above three types as the basis. The main motive behind the cluster interpretation was to provide an insight into the current level of security and compliance of the SaaS system, along with recommendations to improve or maintain the security and compliance status of the SaaS system.

Category A – Governance cluster interpretations

- **Cluster 0**
    - **Insights** – Compliant in SaaS - Identity Management Governance related controls. Low risk of security incidents related to the governance side of the identity management controls within SaaS application.
    - **Recommendations** - Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3.A - Assessing the SaaS cloud Identity Management section, following the proposed 5 step subprocess, and going through the process annually.

- **Cluster 1**
    - **Insights** – Not compliant in SaaS – Identity Management Governance related controls. Critical risk of security incidents related to the governance side of the identity management controls within SaaS applications. Considerable effort is required to improve compliance to Identity Management Governance controls.
    - **Recommendations** – Highly recommend referring to Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3.A - Assessing the SaaS cloud Identity Management section, following the proposed 5 step subprocess, and going through the process annually.

- **Cluster 2**
    - **Insights** – Not compliant with mandatory controls required in the SaaS - Identity Management Governance section and lack complete compliance. Medium to high risk of security incidents related to the governance side of the identity management controls within SaaS application. There is room for improvement in the Identity Management Governance side to better compliance and security.
    - **Recommendations** – Recommend referring Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3.A - Assessing the SaaS cloud Identity Management section, following the proposed 5 step subprocess, and going through the process annually.

Category A – Operations cluster interpretations

- **Cluster 0**
    - **Insights** – Compliant in SaaS - Identity Management Operations related controls. Low risk of security incidents related to the operations side of the identity management controls within SaaS application.
    - **Recommendations** - Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3.A - Assessing the SaaS cloud Identity Management section, following the proposed 5 step subprocess, and going through the process annually.

- **Cluster 1**
    - **Insights** – Not compliant in SaaS – Identity Management Operations related controls. Critical risk of security incidents related to the operations side of the identity management controls within SaaS application. Considerable effort is required to improve compliance to Identity Management Operations controls.
    - **Recommendations** – Highly recommend referring to Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3.A - Assessing the SaaS cloud Identity

Management section, following the proposed 5 step subprocess, and going through the process annually.

- **Cluster 2 & 3**
    - **Insights** – Not compliant with mandatory controls required in the SaaS - Identity Management Operations section and complete lack compliance. Medium to high risk of security incidents related to the operations side of the identity management controls within SaaS application. There is room for improvement in the Identity Management Operations side to better compliance and security.
    - **Recommendations** – Recommend referring Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3.A - Assessing the SaaS cloud Identity Management section, following the proposed 5 step subprocess, and going through the process annually.

Category B – Governance cluster interpretations

- **Cluster 0**
    - **Insights** – Compliant in SaaS - Metastructure Governance related controls. Low risk of security incidents related to the governance side of the metastructure controls within SaaS application.
    - **Recommendations** - Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. B - Assessing the SaaS cloud Metastructure section, following the proposed 5 step subprocess, and going through the process annually.

- **Cluster 1 & 2**
    - **Insights** – Not compliant in SaaS – Metastructure Governance related controls. Critical/ high risk of security incidents related to the operations side of the metastructure controls within SaaS application. Considerable effort is required to improve compliance with Metastructure Operations controls.

- **Recommendations** – Highly recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. B - Assessing the SaaS cloud Metastructure section, following the proposed 5 step subprocess, and going through the process annually.

Category B – Operations cluster interpretations

- **Cluster 0**
  - **Insights** – Compliant in SaaS - Metastructure Operations related controls. Low risk of security incidents related to the operations side of the metastructure within SaaS application.
  - **Recommendations** - Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. B - Assessing the SaaS cloud Metastructure section, following the proposed 5 step subprocess, and going through the process annually.

- **Cluster 1 & 2**
  - **Insights** – Not compliant in SaaS – Metastructure Operations related controls. Critical risk of security incidents related to the operations side of the metastructure controls within SaaS application. Considerable effort is required to improve compliance with Metastructure Operations controls.
  - **Recommendations** – Highly recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. B - Assessing the SaaS cloud Metastructure section, following the proposed 5 step subprocess, and going through the process annually.

Category C – Governance cluster interpretations

- **Cluster 0**
  - **Insights** – Compliant in SaaS - Applistructure & Infostructure Governance related controls. Low risk of security incidents related to the governance side of the Applistructure & Infostructure controls within SaaS application.
  - **Recommendations** - Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. C - Assessing the SaaS cloud Applistructure & Infostructure section, following the proposed 5 step subprocess, and going through the process annually.

- **Cluster 1**
  - **Insights** – Not compliant in SaaS – Applistructure & Infostructure Governance related controls. Critical risk of security incidents related to your SaaS application's Applistructure & Infostructure area. Considerable effort is required to improve compliance to Applistructure & Infostructure Governance controls.
  - **Recommendations** – Highly recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. C - Assessing the SaaS cloud Applistructure & Infostructure section, following the proposed 5 step subprocess, and going through the process annually.

- **Cluster 2**
  - **Insights** – Not compliant with mandatory controls required in the SaaS - Applistructure & Infostructure Governance section and complete lack compliance. Medium to high risk of security incidents related to the governance side of the Applistructure & Infostructure controls within SaaS application. There is room for improvement in the Applistructure & Infostructure Governance side to better compliance and security.
  - **Recommendations** – Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems

consuming public cloud services - 3. C - Assessing the SaaS cloud Applistructure & Infostructure section, following the proposed 5 step subprocess, and going through the process annually.

Category C – Operations cluster interpretations

- **Cluster 0**
  - **Insights** – Compliant in SaaS - Applistructure & Infostructure Operations related controls. Low risk of security incidents related to the operations side of the Applistructure & Infostructure controls within SaaS application.
  - **Recommendations** – Recommend referring to Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. C - Assessing the SaaS cloud Applistructure & Infostructure section, following the proposed 5 step subprocess, and going through the process annually.

- **Cluster 1**
  - **Insights** – Not compliant in SaaS – Applistructure & Infostructure Operations related controls. Critical risk of security incidents related to your SaaS application's Applistructure & Infostructure area. Considerable effort is required to improve compliance to Applistructure & Infostructure Operations controls.
  - **Recommendations** – Highly recommend referring to Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. C - Assessing the SaaS cloud Applistructure & Infostructure section, following the proposed 5 step subprocess, and going through the process annually.

- **Cluster 2, 3 & 4**
  - **Insights** – Not compliant with mandatory controls required in the SaaS - Applistructure & Infostructure Operations section and complete lack compliance. Medium to high risk of security incidents related to the operations side of the Applistructure & Infostructure controls within SaaS application.

There is room for improvement in the Applistructure & Infostructure Operations side to better compliance and security.

- **Recommendations** – Recommend referring to Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. C - Assessing the SaaS cloud Applistructure & Infostructure section, following the proposed 5 step subprocess, and going through the process annually.

Category D – Governance cluster interpretations

- **Cluster 2**
  - **Insights** – Compliant in SaaS - Infrastructure Governance related controls. Low risk of security incidents related to the governance side of the infrastructure controls within SaaS application.
  - **Recommendations** - Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. D - Assessing the SaaS cloud Infrastructure section, following the proposed 5 step subprocess, and going through the process annually.

- **Cluster 3**
  - **Insights** – Not compliant in SaaS – Infrastructure Governance related controls. Critical risk of security incidents related to the Infrastructure area of your SaaS application. Considerable effort is required to improve compliance to Infrastructure Governance controls.
  - **Recommendations** – Highly recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. D - Assessing the SaaS cloud Infrastructure section, following the proposed 5 step subprocess, and going through the process annually.

- **Cluster 0 & 1**
    - **Insights** – Not compliant with mandatory controls required in the SaaS - Infrastructure Governance section and lack complete compliance. Medium to high risk of security incidents related to the governance side of the Infrastructure controls within SaaS application. There is room for improvement in the Infrastructure Governance side to better compliance and security.
    - **Recommendations** – Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. D - Assessing the SaaS cloud Infrastructure section, following the proposed 5 step subprocess, and going through the process annually.

Category D – Operations cluster interpretations

- **Cluster 0**
    - **Insights** – Compliant in SaaS - Infrastructure Operations related controls. Low risk of security incidents related to the operations side of the infrastructure controls within SaaS application.
    - **Recommendations** - Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. D - Assessing the SaaS cloud Infrastructure section, following the proposed 5 step subprocess, and going through the process annually.

- **Cluster 1**
    - **Insights** – Not compliant in SaaS – Infrastructure operations related controls. Critical risk of security incidents related to the Infrastructure area of your SaaS application. Considerable effort is required to improve compliance to Infrastructure Operations controls.
    - **Recommendations** – Highly recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. D - Assessing the SaaS cloud

Infrastructure section, following the proposed 5 step subprocess, and going through the process annually.

- **Cluster 2 & 3**
    - **Insights** – Not compliant with mandatory controls required in the SaaS - Infrastructure Operations section and complete lack compliance. Medium to high risk of security incidents related to the operations side of the Infrastructure controls within SaaS application. There is room for improvement in the Infrastructure Operations side to better compliance and security.
    - **Recommendations** – Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. D - Assessing the SaaS cloud Infrastructure section, following the proposed 5 step subprocess, and going through the process annually.

4.2 - Implementation of the API service

The core focus of this phase of the implementation was to design accessible and efficient ways for security teams and compliance teams to interact with the machine learning models implemented in the above step. As the machine learning model outputs were based on the proposed reference model, the API service will be a gateway for users to interact with the proposed model. With the popularity and adoption of DevSecOps philosophy and practices [54], a solution of this caliber will allow security teams to automate their way of checking their SaaS applications' cloud compliance and security status.

As we have discussed within the Introduction chapter (Chapter 1) and Literature Review chapter (Chapter 2), most startups running at the initial stages are less likely to focus on talent that is primarily specific to security and compliance—so having a solution that provides easy integration and a more familiar way of interaction with the proposed reference model for application developers will be the key for the success of this research and its proposed outcomes for startups at their early stages. Hence this solution will give them a more developer-friendly approach to interacting and getting the best out of the proposed reference model to improve their SaaS cloud security and compliance status.

4.2.1 – High-level architecture of the API service implementation

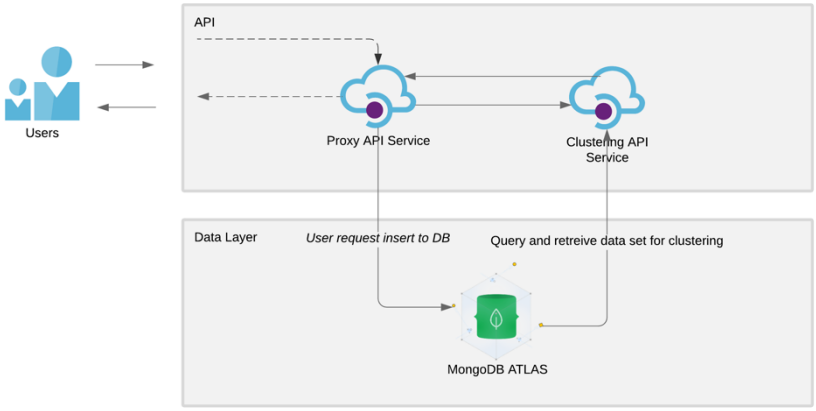


Figure 23 – High-level architecture of API service

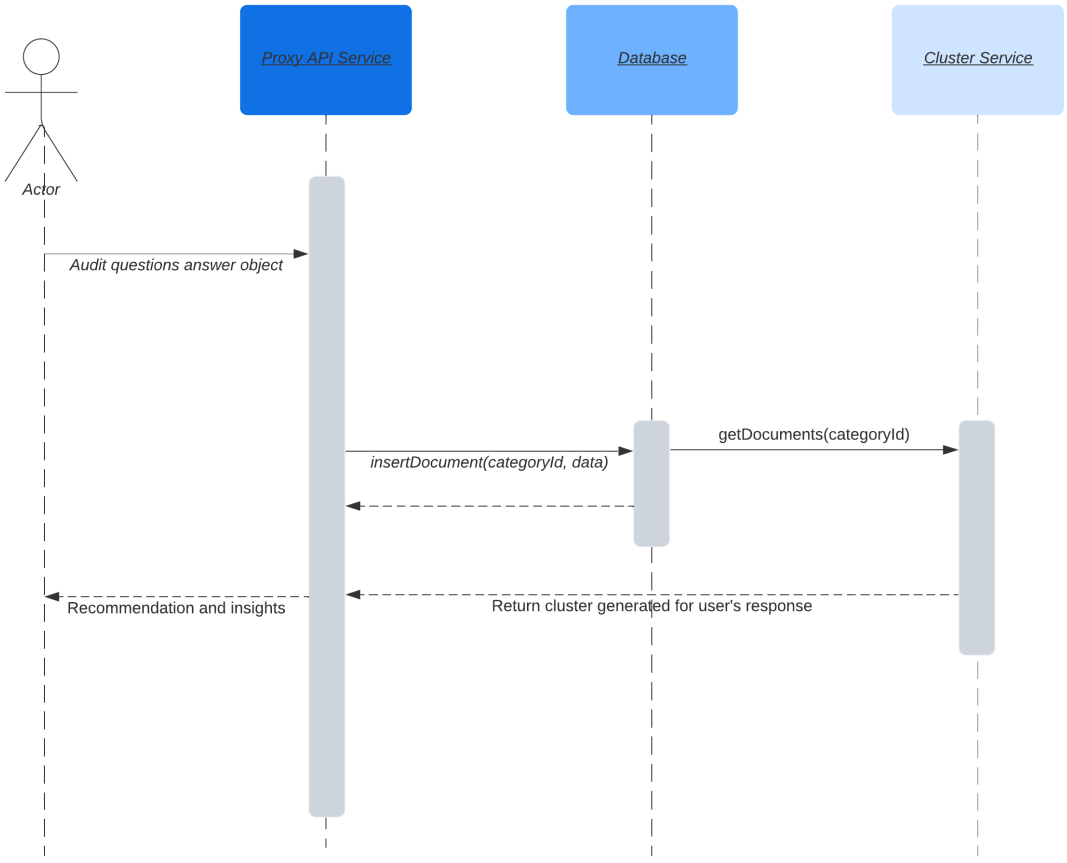


Figure 24 – Sequence diagram of API service

As the high-level architecture diagram and sequence diagram depicts, the API service was designed following microservice architecture principles. The proxy API service will be the

main interaction point for end-users. It exposes eight API POST endpoints designated for each category and passthrough the requests to clustering API service after initial validations. The clustering API service will then perform clustering for the user's data based on the cluster numbers identified in the machine learning model implementation step and return the cluster to which the user's request object belongs. One key thing to note here is that each request object under each category will be stored within that respective category's data collection within the database. The clustering will be done for the whole data set, including the data used for training and the new data. So as more data is collected, the ML model's accuracy and prediction success rate will be expected to grow. After returning the cluster value from the clustering API service, the proxy API service will perform a preprocessing step to add recommendations and insights based on the identified cluster interpretations to the response body. It will also add a score percentage to the request body, which will let users know the score percentage of mandatory audit questions they have answered as Yes within each category (discussed in detail under 4.1.1 – Data collection and organization section). The final response will be returned to the user. All specifics about the final API implementation are presented in the 4.2.4 - API service contract section.

4.2.2 – Selection of technologies/ tools

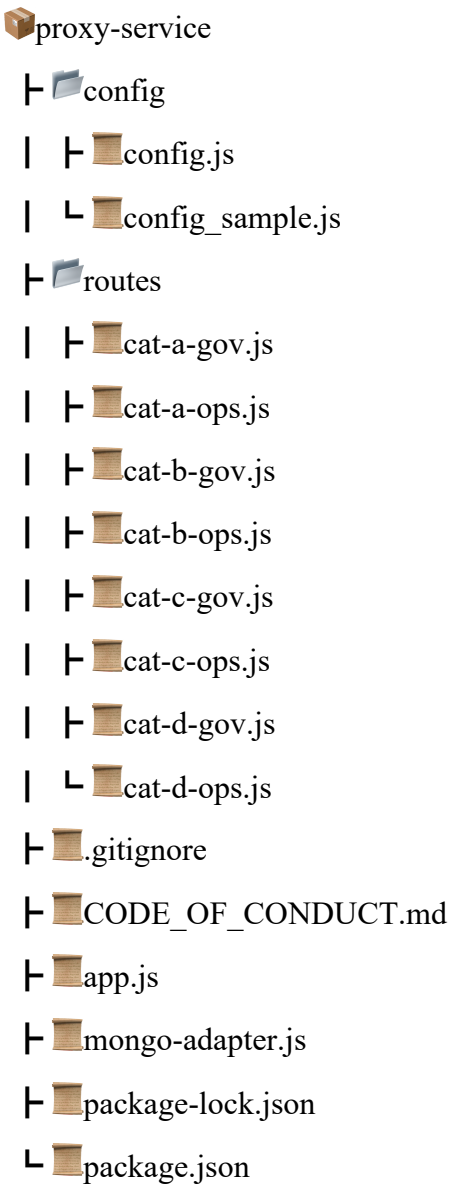
The proxy API service was developed using Node JS as it's considered one of the best runtime environments based on JavaScript programming language. It's also a popular choice in developing microservices-based I/O intensive server-side applications due to its single-threaded nature. The clustering API service was developed using Python. The advantages the python language has for machine learning-based developments were discussed in previous sections. MongoDB, a NoSQL solution, was selected as the database layer for this implementation mainly due to its ability to handle large volumes of data and the easiness of doing updates to the schemas and fields. Also, the scalability and performance factor that MongoDB provides was considered when making this decision.

Express JS was used as the web application framework within Node JS to handle routing within the proxy API service. Flask was used as the web application framework within the clustering API service.

4.2.3 – API service source code and database schema analysis

4.2.3.1 – Proxy API Service

The proxy API service consists of the following folder and file structure.



The following code snippet consists of the source code defined within app.js. It includes the code related to endpoint configurations and Node JS server configurations.

```
1.  var config = require('./config/config');
2.
3.  var express = require('express')
```

```
4.  var http = require('http'),
5.      path = require('path');
6.
7.  var cat_A_Gov = require('./routes/cat-a-gov')
8.  var cat_A_Ops = require('./routes/cat-a-ops')
9.  var cat_B_Gov = require('./routes/cat-b-gov')
10. var cat_B_Ops = require('./routes/cat-b-ops')
11. var cat_C_Gov = require('./routes/cat-c-gov')
12. var cat_C_Ops = require('./routes/cat-c-ops')
13. var cat_D_Gov = require('./routes/cat-d-gov')
14. var cat_D_Ops = require('./routes/cat-d-ops')
15.
16. const mongoAdapter = require('./mongo-adapter')
17. const cors = require('cors')
18. const bodyParser = require('body-parser')
19. var app = express();
20. let port = process.env.PORT || 3001;
21.
22. app.use(cors())
23. app.use(express.json());
24. app.use(express.urlencoded({ extended: true }));
25.
26. app.post('/cat-a-gov', cat_A_Gov.analyizeCatAGovDataCluster);
27. app.post('/cat-a-ops', cat_A_Ops.analyizeCatAOpsDataCluster);
28. app.post('/cat-b-gov', cat_B_Gov.analyizeCatBGovDataCluster);
29. app.post('/cat-b-ops', cat_B_Ops.analyizeCatBOpsDataCluster);
30. app.post('/cat-c-gov', cat_C_Gov.analyizeCatCGovDataCluster);
31. app.post('/cat-c-ops', cat_C_Ops.analyizeCatCOpsDataCluster);
32. app.post('/cat-d-gov', cat_D_Gov.analyizeCatDGovDataCluster);
33. app.post('/cat-d-ops', cat_D_Ops.analyizeCatDOpsDataCluster);
34.
35. app.get('/', (req, res) => {
36.     res.send('Hello World! SaaS Security Compliance Analyzer Proxy API service is
    Live!')
37. });
38.
39. var server = http.createServer(app).listen(port, function () {
40.     console.log(`SaaS Security Compliance Analyzer Proxy API service is listening on
    port ${port}!`)
41.
42.     mongoAdapter.openConnection(function (status) {
43.     });
44. });
45.
46. config.httpServer = server;
47. exports = module.exports = app;
```

The following code snippet only includes the source code within routes/cat-a-gov.js. It consists of the proxy API service handling logic for the Category A – Governance cluster. Other files within the routes folder consist of the handling logic for other respective clusters. The same flow and logic were used within those routes as well. The only changes are the internal variables used. Hence the same source code analysis applies to all the other categories within the routes folder.

Line 9 and 10 include basic validation for the request object. Lines 20 to 31 have the score calculation logic, which will calculate the score percentage for the user's response based on the number of mandatory questions compiled as "Yes". The line starting from 63 includes the final response object, which will be decided based on the returned cluster from the cluster service API.

```
1.  const config = require("../config/config.js"); // Config.js file consists of all the
    configuration details
2.  var mongoAdapter = require("../mongo-adapter"); // Helper module which consists of
    abstracted methods to interact with MongoDB
3.  const http = require('http');
4.
5.  exports.analyizeCatAGovDataCluster = function (req, response) {
6.      var catAGovReqObject = req.body;
7.      console.dir(catAGovReqObject);
8.
9.      if (typeof catAGovReqObject != 'undefined' && catAGovReqObject) {
10.         if (catAGovReqObject.hasOwnProperty('A3') &&
    catAGovReqObject.hasOwnProperty('A4') && catAGovReqObject.hasOwnProperty('A7')) {
11.             mongoAdapter.insertDocument(config.mongodb.collections.CatAGov,
    catAGovReqObject, config.mongodb.centralDB, function(error, doc) {
12.
13.                 if (error) {
14.                     response.writeHead(500, {"Content-Type": "application/json"});
15.                     response.write(JSON.stringify({"message": "Error in communicating
    with the DB"}));
16.                     response.end();
17.                     return;
18.                 }
19.
20.                 // Score Calculation Logic
21.                 var mandatory_questions_ids = ['A3', 'A4'];
22.                 var response_score = 0;
23.
24.                 for (const mandatory_questions_id of mandatory_questions_ids) {
```

```
                    if (catAGovReqObject[mandatory_questions_id].toLowerCase() == "yes")
{
                        response_score++;
                    }
                }

                let final_score_percentage = (response_score /
mandatory_questions_ids.length) * 100;
                final_score_percentage = final_score_percentage.toFixed(0);

                let url = config.apis.clusteringServiceEndpoint + "?category=" +
config.category.CatAGov;

                http.get(url, (res) => {
                    const {statusCode} = res;
                    const contentType = res.headers['content-type'];

                    let error;
                    // Any 2xx status code signals a successful response
                    if (statusCode !== 200) {
                        error = new Error('Request Failed.\n' +
                            `Status Code: ${statusCode}`);
                    } else if (!/^application\/json/.test(contentType)) {
                        error = new Error('Invalid content-type.\n' +
                            `Expected application/json but received ${contentType}`);
                    }

                    if (error) {
                        console.error(error.message);
                        response.writeHead(500, {"Content-Type": "application/json"});
                        response.write(JSON.stringify({"message": "Error in processing
Clustering Service"}));
                        response.end();
                        return;
                    }

                    res.setEncoding('utf8');
                    let rawData = '';
                    res.on('data', (chunk) => {
                        rawData += chunk;
                    });
                    res.on('end', () => {
                        // Final response
                        try {
                            const parsedData = JSON.parse(rawData);
                            console.log(parsedData);
```

```
67.
68.                             var result;
69.
70.                             if (parsedData == "0") {
71.                                 result = JSON.stringify({
72.                                     response: true,
73.                                     code: 200,
74.                                     response_cluster: parsedData,
75.                                     score_percentage: final_score_percentage,
76.                                     insight: config.category.CatAGovBestInsight,
77.                                     recommendation:
    config.category.CatAGovBestRecommendation
78.                                 });
79.
80.                             } else if (parsedData == "1") {
81.                                 result = JSON.stringify({
82.                                     response: true,
83.                                     code: 200,
84.                                     response_cluster: parsedData,
85.                                     score_percentage: final_score_percentage,
86.                                     insight: config.category.CatAGovWorstInsight,
87.                                     recommendation:
    config.category.CatAGovWorstRecommendation
88.                                 });
89.
90.                             } else if (parsedData == "2") {
91.                                 result = JSON.stringify({
92.                                     response: true,
93.                                     code: 200,
94.                                     response_cluster: parsedData,
95.                                     score_percentage: final_score_percentage,
96.                                     insight: config.category.CatAGovMediumInsight,
97.                                     recommendation:
    config.category.CatAGovMediumRecommendation
98.                                 });
99.
100.                            } else {
101.                                response.writeHead(500, {"Content-Type":
    "application/json"});
102.                                response.write(JSON.stringify({"message": "Error in
    returning response analysis"}));
103.                                response.end();
104.                                return;
105.                            }
106.
```

```
                                response.writeHead(200, {"Content-Type":
    "application/json"});
                                response.write(result);
                                response.end();
                                return;

                            } catch (e) {
                                console.error(e.message);
                            }
                        });
                    }).on('error', (e) => {
                        console.error(`Got error: ${e.message}`);
                    });
                });

            } else {
                response.writeHead(400, {"Content-Type": "application/json"});
                response.write(JSON.stringify({"message": "Required Parameters for
    Category A - Governance are not defined"}));
                response.end();
                return;
            }

        } else {
            response.writeHead(400, {"Content-Type": "application/json"});
            response.write(JSON.stringify({"message": "Required Payload for Category A -
    Governance not defined"}));
            response.end();
            return;
        }
    };
```

4.2.3.2 – Clustering API Service

The clustering API service consists of the following folder and file structure.

The following code snippet consists of the source code defined within the app.py file. It includes the entry point of the clustering API service, which will return the derived cluster value to the user response under each category. The clustering API service /response-cluster GET method expects the category name as a query parameter.

```
1.  import flask
2.  from flask import request, jsonify
3.  from main import ML
4.  from flask import request
5.
6.  app = flask.Flask(__name__)
7.  app.config["DEBUG"] = True
8.
9.  @app.route('/response-cluster', methods=['GET'])
10. def home():
11.     category = request.args.get('category', default="CatAGov", type=str)
12.     cluster = ML.cluster_response(self=ML, category=category)
13.     print(cluster[0])
14.     return jsonify(str(cluster[0]))
15.
16. app.run()
```

The following code snippet includes the source code defined within the main.py file. It includes the clustering functionality defined within class ML. All the code were reused from the machine learning model implementation phase. The k (cluster) value for the KModes algorithm was defined based on the cluster values derived in the implementation phase.

```
1.  import urllib
2.  from pymongo import MongoClient
3.  from sklearn import preprocessing
4.  from kmodes.kmodes import KModes
5.  import numpy as np
6.  import pandas as pd
7.  pd.set_option('display.max_colwidth', 500)
8.
9.  class ML:
10.
11.     def cluster_response(self, category):
12.         client = MongoClient("<MongoDB-Conn-URL>")
13.         db = client["saas_sca"]
```

```
14.         collection = db[category]
15.
16.         df = pd.DataFrame(list(collection.find({})))
17.         print(df.head())
18.
19.         df_copy = df.copy()
20.         del df['_id']
21.
22.         df.shape
23.         df.describe()
24.         df.info()
25.         df.isnull().sum()*100/df.shape[0] # Checking for null values
26.
27.         # Label Encoding process
28.         df.replace(np.nan, 'notapplicable', inplace=True)
29.         le = preprocessing.LabelEncoder()
30.         df = df.apply(le.fit_transform)
31.
32.         # KModes Clustering - Cluster number is decided based on the trainning data
    derived values
33.         k_value_mapper_for_clusters = {
34.             "CatAGov": 3,
35.             "CatAOps": 4,
36.             "CatBGov": 3,
37.             "CatBOps": 3,
38.             "CatCGov": 3,
39.             "CatCOps": 5,
40.             "CatDGov": 4,
41.             "CatDOps": 4
42.         }
43.
44.         k = k_value_mapper_for_clusters.get(category)
45.
46.         # KModes with Cao Initialization
47.         km_cao = KModes(n_clusters=k, init = "Cao", n_init = 1, verbose=1)
48.         fit_clusters_cao = km_cao.fit_predict(df)
49.
50.         df['Predicted_Cluster'] = fit_clusters_cao
51.
52.         response_cluster = df['Predicted_Cluster'].tail(1).values
53.
54.         return response_cluster
```

4.2.3.3 – Database schema

The MongoDB database consists of 8 total collections, where each collection was used to store data related to each category. The schema design for each collection was pretty straightforward as there weren't any relationship mappings involved between entities. The following snippets present the schema for data about categories and a sample category object, respectively. Please note that the given schema and object definitions are related to Category A – Governance. The exact format was used to define schema and object definition for other categories.

```
1.  {
2.      "title": "CatAGov”
3.      "required": [
4.          "_id",
5.          "A3",
6.          "A4",
7.          "A7"
8.      ],
9.      "properties": {
10.         "_id": {
11.             "bsonType": "objectId"
12.         },
13.         "A3": {
14.             "bsonType": "string"
15.         },
16.         "A4": {
17.             "bsonType": "string"
18.         },
19.         "A7": {
20.             "bsonType": "string"
21.         }
22.     }
23. }
```

```
1.  {
2.      "_id": ObjectId("61de469e9e6b07736ebfe588"),
3.      "A3": "Yes",
4.      "A4": "Yes",
5.      "A7": "Yes"
6.  }
```

4.2.4 – API service contract

This section presents the API service documentation for the proxy service API as the end-user will be interacting with it. API service endpoints are divided based on the categories. None of the API endpoints accepts any query parameters.

4.2.4.1 – API contract for Category A – Governance

Table 9 – API details for Category A - Governance

API endpoint	{domain}/cat-a-gov
Supported methods	POST
Headers	Content-Type: application/json

Expected Request Object	{
	A3: 'Yes',
	A4: 'Yes',
	A7: 'Yes'
	}

Response Specifications

Response Codes

- 200 - Success
- 400 – Client-Side Error
- 500 - Server Side Error

Table 10 – API response details for Category A – Governance ***(Spans across multiple pages)***

Response Code	Response Object	Reason
400	{ message: "Required Payload for Category A - Governance not defined"	The payload object is not defined in the request.

	}	

400	{
	message: "Required Parameters for Category A - Governance are not defined"
	}
		Required parameters aren't defined according to the expected request object format.

500	{
	message: "Error in communicating with the DB"
	}
		Internal Error in adding the user request object to DB.

500	{
	message: "Error in processing Clustering Service"
	}
		Internal Error in communicating with the clustering API service.

500	{
	message: "Error in returning response analysis"
	}
		Internal Error in returning response analysis.

200	{ "response": true, "code": 200, "response_cluster": "0", "score_percentage": "100", "insight": "Compliant in SaaS - Identity Management Governance related controls. Low risk of security incidents related to the governance side of the identity management controls within SaaS application.", "recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems	Successful response for a request object belonging to cluster interpretation of type 1.

	consuming public cloud services - 3.A - Assessing the SaaS cloud Identity Management section, following the proposed 5 step subprocess, and going through the process annually." }	

200	{
	"response": true,
	"code": 200,
	"response_cluster": "1",
	"score_percentage": "50",
	"insight": "Not compliant in SaaS – Identity Management Governance related controls. Critical risk of security incidents related to the governance side of the identity management controls within SaaS applications. Considerable effort is required to improve compliance to Identity Management Governance controls.",
	"recommendation": "Highly recommend referring to Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3.A - Assessing the SaaS cloud Identity Management section, following the proposed 5 step subprocess, and going through the process annually."
	}
		Successful response for a request object belonging to cluster interpretation of type 2.

200	{ "response": true, "code": 200, "response_cluster": "2", "score_percentage": "0",	Successful response for a request object belonging to cluster interpretation of type 3.

	"insight": "Not compliant with mandatory controls required in the SaaS - Identity Management Governance section and lack complete compliance. Medium to high risk of security incidents related to the governance side of the identity management controls within SaaS application. There is room for improvement in the Identity Management Governance side to better compliance and security.", "recommendation": "Recommend referring Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3.A - Assessing the SaaS cloud Identity Management section, following the proposed 5 step subprocess, and going through the process annually." }	

4.2.4.2 – API contract for Category A – Operations

Table 11 – API details for Category A - Operations

API endpoint	{domain}/cat-a-ops
Supported methods	POST
Headers	Content-Type: application/json

Expected Request Object	{
	A1: 'Yes',
	A2: 'Yes',
	A5: 'Yes',
	A6: 'Yes',
	A8: 'Yes',
	A9: 'Yes'
	}

Response Specifications

Response Codes

- 200 - Success
- 400 – Client-Side Error
- 500 - Server Side Error

Table 12 – API response details for Category A – Operations *(Spans across multiple pages)*

Response Code	**Response Object**	**Reason**

400	{
	message: "Required Payload for Category A - Operations not defined"
	}
		The payload object is not defined in the request.

400	{
	message: "Required Parameters for Category A - Operations are not defined"
	}
		Required parameters aren't defined according to the expected request object format.

500	{
	message: "Error in communicating with the DB"
	}
		Internal Error in adding the user request object to DB.

500	{
	message: "Error in processing Clustering Service"
	}
		Internal Error in communicating with the clustering API service.

500	{ message: "Error in returning response analysis"	Internal Error in returning response analysis.

	}	

200	{
	"response": true,
	"code": 200,
	"response_cluster": "0",
	"score_percentage": "100",
	"insight": "Compliant in SaaS - Identity Management Operations related controls. Low risk of security incidents related to the operations side of the identity management controls within SaaS application.",
	"recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3.A - Assessing the SaaS cloud Identity Management section, following the proposed 5 step subprocess, and going through the process annually."
	}
		Successful response for a request object belonging to cluster interpretation of type 1.

200	{ "response": true, "code": 200, "response_cluster": "1", "score_percentage": "20", "insight": "Not compliant in SaaS – Identity Management Operations related controls. Critical risk of security incidents related to the operations side of the identity management controls within SaaS application. Considerable effort is required to improve compliance to Identity Management Operations controls.",	Successful response for a request object belonging to cluster interpretation of type 2.

	"recommendation": "Highly recommend referring to Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3.A - Assessing the SaaS cloud Identity Management section, following the proposed 5 step subprocess, and going through the process annually." }	

200	{
	"response": true,
	"code": 200,
	"response_cluster": "3",
	"score_percentage": "40",
	"insight": "Not compliant with mandatory controls required in the SaaS - Identity Management Operations section and complete lack compliance. Medium to high risk of security incidents related to the operations side of the identity management controls within SaaS application. There is room for improvement in the Identity Management Operations side to better compliance and security.",
	"recommendation": "Recommend referring Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3.A - Assessing the SaaS cloud Identity Management section, following the proposed 5 step subprocess, and going through the process annually."
	}
		Successful response for a request object belonging to cluster interpretation of type 3.

4.2.4.3 – API contract for Category B – Governance

Table 13 – API details for Category B – Governance

API endpoint	{domain}/cat-b-gov
Supported methods	POST
Headers	Content-Type: application/json

Expected Request Object	{
	B3: 'Yes',
	B4: 'Yes',
	B5: 'Yes',
	B6: 'Yes',
	B7: 'Yes',
	B8: 'Yes',
	B11: 'Yes',
	B13: 'Yes',
	B14: 'Yes',
	B15: 'Yes',
	B17: 'Yes',
	B21: 'Yes',
	B22: 'Yes',
	B23: 'Yes',
	B24: 'Yes',
	B25: 'Yes'
	}

Response Specifications

Response Codes

- 200 - Success
- 400 – Client-Side Error
- 500 - Server Side Error

Table 14 – API response details for Category B – Governance *(Spans across multiple pages)*

Response Code	**Response Object**	**Reason**

400	{
	message: "Required Payload for Category B - Governance not defined"
	}
		The payload object is not defined in the request.

400	{
	message: "Required Parameters for Category B - Governance are not defined"
	}
		Required parameters aren't defined according to the expected request object format.

500	{
	message: "Error in communicating with the DB"
	}
		Internal Error in adding the user request object to DB.

500	{
	message: "Error in processing Clustering Service"
	}
		Internal Error in communicating with the clustering API service.

500	{
	message: "Error in returning response analysis"
	}
		Internal Error in returning response analysis.

200	{ "response": true, "code": 200, "response_cluster": "0", "score_percentage": "100",	Successful response for a request object belonging to cluster interpretation of type 1.

	"insight": "Compliant in SaaS - Metastructure Governance related controls. Low risk of security incidents related to the governance side of the metastructure controls within SaaS application.", "recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. B - Assessing the SaaS cloud Metastructure section, following the proposed 5 step subprocess, and going through the process annually." }	
200	{ "response": true, "code": 200, "response_cluster": "1", "score_percentage": "33", "insight": "Not compliant in SaaS – Metastructure Governance related controls. Critical/ high risk of security incidents related to the operations side of the metastructure controls within SaaS application. Considerable effort is required to improve compliance with Metastructure Operations controls.", "recommendation": "Highly recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. B - Assessing the SaaS cloud Metastructure section, following the proposed 5 step subprocess, and going through the process annually."	Successful response for a request object belonging to cluster interpretation of type 2.

	}	

4.2.4.4 – API contract for Category B – Operations

Table 15 – API details for Category B – Operations

API endpoint	{domain}/cat-b-ops
Supported methods	POST
Headers	Content-Type: application/json

Expected Request Object	{
	B1: 'N/A',
	B2: 'Yes',
	B9: 'Yes',
	B10: 'Yes',
	B12: 'Yes',
	B16: 'Yes',
	B18: 'No',
	B19: 'Yes',
	B20: 'Yes'
	}

Response Specifications

Response Codes

- 200 - Success
- 400 – Client-Side Error
- 500 - Server Side Error

Table 16 – API response details for Category B – Operations *(Spans across multiple pages)*

Response Code	**Response Object**	**Reason**

400	{
	message: "Required Payload for Category B - Operations not defined"
	}
		The payload object is not defined in the request.

400	{
	message: "Required Parameters for Category B - Operations are not defined"
	}
		Required parameters aren't defined according to the expected request object format.

500	{
	message: "Error in communicating with the DB"
	}
		Internal Error in adding the user request object to DB.

500	{
	message: "Error in processing Clustering Service"
	}
		Internal Error in communicating with the clustering API service.

500	{
	message: "Error in returning response analysis"
	}
		Internal Error in returning response analysis.

200	{ "response": true, "code": 200, "response_cluster": "0", "score_percentage": "100",	Successful response for a request object belonging to cluster interpretation of type 1.

	"insight": "Compliant in SaaS - Metastructure Operations related controls. Low risk of security incidents related to the operations side of the metastructure within SaaS application.", "recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. B - Assessing the SaaS cloud Metastructure section, following the proposed 5 step subprocess, and going through the process annually." }	

200	{
	"response": true,
	"code": 200,
	"response_cluster": "1",
	"score_percentage": "0",
	"insight": "Not compliant in SaaS – Metastructure Operations related controls. Critical risk of security incidents related to the operations side of the metastructure controls within SaaS application. Considerable effort is required to improve compliance with Metastructure Operations controls.",
	"recommendation": "Highly recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. B - Assessing the SaaS cloud Metastructure section, following the proposed 5 step subprocess, and going through the process annually."
	}
		Successful response for a request object belonging to cluster interpretation of type 2.

200	{
	"response": true,
	"code": 200,
	"response_cluster": "2",
	"score_percentage": "33",
	"insight": "Not compliant with mandatory controls required in the SaaS - Metastructure Operations section and lack complete compliance. Medium to high risk of security incidents related to the operations side of the metastructure controls within SaaS application. There is room for improvement in the Metastructure Operations side to better compliance and security.",
	"recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. B - Assessing the SaaS cloud Metastructure section, following the proposed 5 step subprocess, and going through the process annually."
	}
		Successful response for a request object belonging to cluster interpretation of type 3.

4.2.4.5 – API contract for Category C – Governance

Table 17 – API details for Category C – Governance

API endpoint	{domain}/cat-c-gov
Supported methods	POST
Headers	Content-Type: application/json
Expected Request Object	{ C3: 'Yes', C4: 'Yes', C5: 'Yes',

	C8: 'Yes', C9: 'Yes', C10: 'Yes' }

Response Specifications

Response Codes

- 200 - Success
- 400 – Client-Side Error
- 500 - Server Side Error

Table 18 – API response details for Category B – Operations ***(Spans across multiple pages)***

Response Code	**Response Object**	**Reason**

400	{
	message: "Required Payload for Category C - Governance not defined"
	}
		The payload object is not defined in the request.

400	{
	message: "Required Parameters for Category C - Governance are not defined"
	}
		Required parameters aren't defined according to the expected request object format.

500	{
	message: "Error in communicating with the DB"
	}
		Internal Error in adding the user request object to DB.

500	{ message: "Error in processing Clustering Service"	Internal Error in communicating with the clustering API service.

	}	

500	{
	message: "Error in returning response analysis"
	}
		Internal Error in returning response analysis.

200	{
	"response": true,
	"code": 200,
	"response_cluster": "0",
	"score_percentage": "100",
	"insight": "Compliant in SaaS - Applistructure & Infostructure Governance related controls. Low risk of security incidents related to the governance side of the Applistructure & Infostructure controls within SaaS application.",
	"recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. C - Assessing the SaaS cloud Applistructure & Infostructure section, following the proposed 5 step subprocess, and going through the process annually."
	}
		Successful response for a request object belonging to cluster interpretation of type 1.

200	{ "response": true, "code": 200, "response_cluster": "1", "score_percentage": "40", "insight": "Not compliant in SaaS – Applistructure & Infostructure Governance related controls. Critical risk of security incidents related to	Successful response for a request object belonging to cluster interpretation of type 2.

	your SaaS application's Applistructure & Infostructure area. Considerable effort is required to improve compliance to Applistructure & Infostructure Governance controls.", "recommendation": "Highly recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. C - Assessing the SaaS cloud Applistructure & Infostructure section, following the proposed 5 step subprocess, and going through the process annually." }	
200	{ "response": true, "code": 200, "response_cluster": "2", "score_percentage": "40", "insight": "Not compliant with mandatory controls required in the SaaS - Applistructure & Infostructure Governance section and complete lack compliance. Medium to high risk of security incidents related to the governance side of the Applistructure & Infostructure controls within SaaS application. There is room for improvement in the Applistructure & Infostructure Governance side to better compliance and security.", "recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. C - Assessing the SaaS cloud Applistructure & Infostructure	Successful response for a request object belonging to cluster interpretation of type 3.

	section, following the proposed 5 step subprocess, and going through the process annually." }	

4.2.4.6 – API contract for Category C – Operations

Table 19 – API details for Category C – Operations

API endpoint	{domain}/cat-c-ops
Supported methods	POST
Headers	Content-Type: application/json

Expected Request Object	{
	C1: 'Yes',
	C2: 'Yes',
	C6: 'Yes',
	C7: 'Yes'
	}

Response Specifications

Response Codes

- 200 - Success
- 400 – Client-Side Error
- 500 - Server Side Error

Table 20 – API response details for Category C – Operations ***(Spans across multiple pages)***

Response Code	**Response Object**	**Reason**
400	{ message: "Required Payload for Category C - Operations not defined"	The payload object is not defined in the request.

	}	

400	{
	message: "Required Parameters for Category A - Operations are not defined"
	}
		Required parameters aren’t defined according to the expected request object format.

500	{
	message: "Error in communicating with the DB"
	}
		Internal Error in adding the user request object to DB.

500	{
	message: "Error in processing Clustering Service"
	}
		Internal Error in communicating with the clustering API service.

500	{
	message: "Error in returning response analysis"
	}
		Internal Error in returning response analysis.

200	{ "response": true, "code": 200, "response_cluster": "0", "score_percentage": "100", "insight": "Compliant in SaaS - Applistructure & Infostructure Operations related controls. Low risk of security incidents related to the operations side of the Applistructure & Infostructure controls within SaaS application.", "recommendation": "Recommend referring to Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems	Successful response for a request object belonging to cluster interpretation of type 1.

	consuming public cloud services - 3. C - Assessing the SaaS cloud Applistructure & Infostructure section, following the proposed 5 step subprocess, and going through the process annually." }	

200	{
	"response": true,
	"code": 200,
	"response_cluster": "1",
	"score_percentage": "25",
	"insight": "Not compliant in SaaS – Applistructure & Infostructure Operations related controls. Critical risk of security incidents related to your SaaS application's Applistructure & Infostructure area. Considerable effort is required to improve compliance to Applistructure & Infostructure Operations controls.",
	"recommendation": "Highly recommend referring to Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. C - Assessing the SaaS cloud Applistructure & Infostructure section, following the proposed 5 step subprocess, and going through the process annually."
	}
		Successful response for a request object belonging to cluster interpretation of type 2.

200	{ "response": true, "code": 200, "response_cluster": "2", "score_percentage": "50",	Successful response for a request object belonging to cluster interpretation of type 3.

	"insight": "Not compliant with mandatory controls required in the SaaS - Applistructure & Infostructure Operations section and complete lack compliance. Medium to high risk of security incidents related to the operations side of the Applistructure & Infostructure controls within SaaS application. There is room for improvement in the Applistructure & Infostructure Operations side to better compliance and security.", "recommendation": "Recommend referring to Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. C - Assessing the SaaS cloud Applistructure & Infostructure section, following the proposed 5 step subprocess, and going through the process annually." }	

4.2.4.7 – API contract for Category D – Governance

Table 21 – API details for Category D – Governance

API endpoint	{domain}/cat-d-gov
Supported methods	POST
Headers	Content-Type: application/json

Expected Request Object	{
	D2: 'Yes',
	D7: 'Yes'
	}

Response Specifications

Response Codes

- 200 - Success
- 400 – Client-Side Error
- 500 - Server Side Error

Table 22 – API response details for Category D – Governance *(Spans across multiple pages)*

Response Code	Response Object	Reason

400	{
	message: "Required Payload for Category D - Governance not defined"
	}
		The payload object is not defined in the request.

400	{
	message: "Required Parameters for Category D - Governance are not defined"
	}
		Required parameters aren't defined according to the expected request object format.

500	{
	message: "Error in communicating with the DB"
	}
		Internal Error in adding the user request object to DB.

500	{
	message: "Error in processing Clustering Service"
	}
		Internal Error in communicating with the clustering API service.

500	{ message: "Error in returning response analysis"	Internal Error in returning response analysis.

	}	

200	{
	"response": true,
	"code": 200,
	"response_cluster": "2",
	"score_percentage": "100",
	"insight": "Compliant in SaaS - Infrastructure Governance related controls. Low risk of security incidents related to the governance side of the infrastructure controls within SaaS application.",
	"recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. D - Assessing the SaaS cloud Infrastructure section, following the proposed 5 step subprocess, and going through the process annually."
	}
		Successful response for a request object belonging to cluster interpretation of type 1.

200	{ "response": true, "code": 200, "response_cluster": "3", "score_percentage": "0", "insight": "Not compliant in SaaS – Infrastructure Governance related controls. Critical risk of security incidents related to the Infrastructure area of your SaaS application. Considerable effort is required to improve compliance to Infrastructure Governance controls.",	Successful response for a request object belonging to cluster interpretation of type 2.

	"recommendation": "Highly recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. D - Assessing the SaaS cloud Infrastructure section, following the proposed 5 step subprocess, and going through the process annually." }	

200	{
	"response": true,
	"code": 200,
	"response_cluster": "0",
	"score_percentage": "50",
	"insight": "Not compliant with mandatory controls required in the SaaS - Infrastructure Governance section and lack complete compliance. Medium to high risk of security incidents related to the governance side of the Infrastructure controls within SaaS application. There is room for improvement in the Infrastructure Governance side to better compliance and security.",
	"recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. D - Assessing the SaaS cloud Infrastructure section, following the proposed 5 step subprocess, and going through the process annually."
	}
		Successful response for a request object belonging to cluster interpretation of type 3.

4.2.4.8 – API contract for Category D – Operations

Table 23 – API details for Category D – Operations

API endpoint	{domain}/cat-d-ops
Supported methods	POST
Headers	Content-Type: application/json

Expected Request Object	{
	D1: 'Yes',
	D3: 'Yes',
	D4: 'Yes',
	D5: 'Yes',
	D6: 'Yes',
	D8: 'Yes',
	D9: 'Yes'
	}

Response Specifications

Response Codes

- 200 - Success
- 400 – Client-Side Error
- 500 - Server Side Error

Table 24 – API response details for Category D – Operations *(Spans across multiple pages)*

Response Code	Response Object	Reason

400	{
	message: "Required Payload for Category D - Operations not defined"
	}
		The payload object is not defined in the request.

400	{
	message: "Required Parameters for Category A - Operations are not defined"
	}
		Required parameters aren't defined according to the expected request object format.

500	{
	message: "Error in communicating with the DB"
	}
		Internal Error in adding the user request object to DB.

500	{
	message: "Error in processing Clustering Service"
	}
		Internal Error in communicating with the clustering API service.

500	{
	message: "Error in returning response analysis"
	}
		Internal Error in returning response analysis.

200	{ "response": true, "code": 200, "response_cluster": "0", "score_percentage": "100", "insight": "Compliant in SaaS - Infrastructure Operations related controls. Low risk of security incidents related to the operations side of the infrastructure controls within SaaS application.", "recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. D - Assessing the SaaS cloud Infrastructure section, following the	Successful response for a request object belonging to cluster interpretation of type 1.

	proposed 5 step subprocess, and going through the process annually." }	

200	{
	"response": true,
	"code": 200,
	"response_cluster": "1",
	"score_percentage": "0",
	"insight": "Not compliant in SaaS – Infrastructure operations related controls. Critical risk of security incidents related to the Infrastructure area of your SaaS application. Considerable effort is required to improve compliance to Infrastructure Operations controls.",
	"recommendation": "Highly recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. D - Assessing the SaaS cloud Infrastructure section, following the proposed 5 step subprocess, and going through the process annually."
	}
		Successful response for a request object belonging to cluster interpretation of type 2.

200	{ "response": true, "code": 200, "response_cluster": "3", "score_percentage": "17", "insight": "Not compliant with mandatory controls required in the SaaS - Infrastructure Operations section and complete lack compliance. Medium to high risk of security incidents related to	Successful response for a request object belonging to cluster interpretation of type 3.

	the operations side of the Infrastructure controls within SaaS application. There is room for improvement in the Infrastructure Operations side to better compliance and security.", "recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. D - Assessing the SaaS cloud Infrastructure section, following the proposed 5 step subprocess, and going through the process annually." }	

4.3 – Mapping of the core components of the proposed reference model with the NIST 800-53 R5

Since we have already mapped core components of the proposed reference model to CSA CSM v3.0.1, the controls of the proposed reference model can be directly mapped to NIST 800-53 R3 and R4 versions. Hence the mapping has been generated based on a direct mapping published between the latest NIST 800-53 R5 the R4 versions [55]. This can be accessed in Appendix L.

4.4 – Conclusive Remarks

The key focus of this chapter was presenting the details related to the implementation phase carried out within this research. The main focus of the implementation phase was to create a way for emerging SaaS business users to interact with the proposed reference model. Aligning with the research objectives, this implementation had to be a way of showcasing how the proposed reference model could be used efficiently in the real world. The initial part of the chapter focused on discussing the background related to the implementation phase. It was followed with a detailed analysis on how the implementation phase was carried out. The chapter was organized into three main subsections, where each subsection included details of

crucial components of the final implementation. Under each section, in-depth details were presented and discussed. It included the process involved, issues faced, and final analysis on how each of those components aligns with the final implementation outcome and the research objectives.

5 – ANALYSIS AND FINDINGS

5.1 – Analysis

This section presents the analysis and the observations of the final implementation. The analysis phase was designed to identify whether the implemented API service and the machine learning models provide the expected outcomes based on the proposed reference model.

The most practical way to analyze the implementation outcomes was by testing the API service by interacting with it in a way that external consumers would do. To do that, different user personas that could interact with this API service were first identified. Then the test scenarios were developed based on that. Each of these test scenarios was designed by taking different user personas into account. The categorization of the test scenarios was done by taking a bottom-up approach and identifying different user responses based on their persona. The following test scenarios were developed based on the above factors.

- Scenario 1 – A user responds “Yes” to all the audit questions within the specified category.
- Scenario 2 – A user responds “No” to all the audit questions within the specified category.
- Scenario 3 – A user responds “Yes” to all mandatory questions and “No” to all non-mandatory questions.
- Scenario 4 – A user responds “No” to all mandatory questions and “Yes” to all non-mandatory questions.
- Scenario 5 – A user responds “Yes” to all mandatory questions and “N/A” to all non-mandatory questions.
- Scenario 6 – A user responds “No” to all mandatory questions and “N/A” to all non-mandatory questions.
- Scenario 7 – A user responds “Yes” to 50% of the total mandatory questions, “No” to 50% of mandatory questions and “N/A” to all non-mandatory questions. (If the mandatory questions are not even, a significant percentage of total mandatory questions were taken as “No” responses)

The table 25 includes analysis of the test scenario results. Each seven different test scenarios mentioned above were carried out in every eight categories introduced in 4.1.2 – Feature selection for the machine learning model section. Some scenarios were left out within categories that didn't include any non-mandatory questions.

Table 25 – Test scenario analysis of the implementation *(Spans across multiple pages)*

Category/ Scenario	**Request Object**	**Response Object**	**Expected outcome achieved (Yes/ No)**
Category A – Gov/ Scenario 1	1. { 2. A3: 'Yes', 3. A4: 'Yes', 4. A7: 'Yes' 5. }	1. { 2. "response": true, 3. "code": 200, 4. "response_cluster": "0", 5. "score_percentage": "100", 6. "insight": "Compliant in SaaS - Identity Management Governance related controls. Low risk of security incidents related to the governance side of the identity management controls within SaaS application.", 7. "recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3.A - Assessing the SaaS cloud Identity Management section, following the proposed 5 step subprocess, and going through the process annually."	Yes

		<pre>8. }</pre>	

Category A – Gov/ Scenario 2	<pre>1. {
	2. A3: 'No',
	3. A4: 'No',
	4. A7: 'No'
	5. }</pre>
		<pre>1. {
		2. "response": true,
		3. "code": 200,
		4. "response_cluster": "1",
		5. "score_percentage": "0",
		6. "insight": "Not compliant in SaaS – Identity Management Governance related controls. Critical risk of security incidents related to the governance side of the identity management controls within SaaS applications. Considerable effort is required to improve compliance to Identity Management Governance controls.",
		7. "recommendation": "Highly recommend referring to Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3.A - Assessing the SaaS cloud Identity Management section, following the proposed 5 step subprocess, and going through the process annually."
		8. }</pre>
			Yes

Category A – Gov/ Scenario 3	<pre>1. {
	2. A3: 'Yes',
	3. A4: 'Yes',
	4. A7: 'No'
	5. }</pre>
		<pre>1. {
		2. "response": true,
		3. "code": 200,
		4. "response_cluster": "0",
		5. "score_percentage": "100",</pre>
			Yes

			<pre>6. "insight": "Compliant in SaaS - Identity Management Governance related controls. Low risk of security incidents related to the governance side of the identity management controls within SaaS application.",
			7. "recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3.A - Assessing the SaaS cloud Identity Management section, following the proposed 5 step subprocess, and going through the process annually."
			8. }</pre>	

Category A – Gov/ Scenario 4	<pre>1. {
	2. A3: 'No',
	3. A4: 'No',
	4. A7: 'Yes'
	5. }</pre>
			<pre>1. {
			2. "response": true,
			3. "code": 200,
			4. "response_cluster": "1",
			5. "score_percentage": "0",
			6. "insight": "Not compliant in SaaS – Identity Management Governance related controls. Critical risk of security incidents related to the governance side of the identity management controls within SaaS applications. Considerable effort is required to improve compliance to Identity Management Governance controls.",</pre>
				Yes

			<pre>"recommendation": "Highly recommend referring to Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3.A - Assessing the SaaS cloud Identity Management section, following the proposed 5 step subprocess, and going through the process annually."
			}</pre>	

Category A – Gov/ Scenario 5	<pre>{
	A3: 'Yes',
	A4: 'Yes',
	A7: 'N/A'
	}</pre>
			<pre>{
			"response": true,
			"code": 200,
			"response_cluster": "0",
			"score_percentage": "100",
			"insight": "Compliant in SaaS - Identity Management Governance related controls. Low risk of security incidents related to the governance side of the identity management controls within SaaS application.",
			"recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3.A - Assessing the SaaS cloud Identity Management section, following the proposed 5 step subprocess, and going</pre>
				Yes

		<pre>through the process annually."
		}</pre>	

Category A – Gov/ Scenario 6	<pre>{
	A3: 'No',
	A4: 'No',
	A7: 'N/A'
	}</pre>
		<pre>{
		"response": true,
		"code": 200,
		"response_cluster": "1",
		"score_percentage": "0",
		"insight": "Not compliant in SaaS – Identity Management Governance related controls. Critical risk of security incidents related to the governance side of the identity management controls within SaaS applications. Considerable effort is required to improve compliance to Identity Management Governance controls.",
		"recommendation": "Highly recommend referring to Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3.A - Assessing the SaaS cloud Identity Management section, following the proposed 5 step subprocess, and going through the process annually."
		}</pre>
			Yes

Category A – Gov/ Scenario 7	<pre>{
	A3: 'No',
	A4: 'Yes',
	A7: 'N/A'</pre>
		<pre>{
		"response": true,
		"code": 200,
		"response_cluster": "2",</pre>
			Yes

	<pre>5. }</pre>		<pre>5. "score_percentage": "50",
			6. "insight": "Not compliant with mandatory controls required in the SaaS - Identity Management Governance section and lack complete compliance. Medium to high risk of security incidents related to the governance side of the identity management controls within SaaS application. There is room for improvement in the Identity Management Governance side to better compliance and security.",
			7. "recommendation": "Recommend referring Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3.A - Assessing the SaaS cloud Identity Management section, following the proposed 5 step subprocess, and going through the process annually."
			8. }</pre>	

Category A – Ops/ Scenario 1	<pre>1. {
	2. A1: 'Yes',
	3. A2: 'Yes',
	4. A5: 'Yes',
	5. A6: 'Yes',
	6. A8: 'Yes',
	7. A9: 'Yes'
	8. }
	9.</pre>
			<pre>1. {
			2. "response": true,
			3. "code": 200,
			4. "response_cluster": "0",
			5. "score_percentage": "100",
			6. "insight": "Compliant in SaaS - Identity Management Operations related controls. Low risk of security incidents related to the operations side of</pre>
				Yes

			<pre>the identity management controls within SaaS application.",
			7. "recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3.A - Assessing the SaaS cloud Identity Management section, following the proposed 5 step subprocess, and going through the process annually."
			8. }</pre>	

Category A – Ops/ Scenario 2	<pre>1. {
	2. A1: 'No',
	3. A2: 'No',
	4. A5: 'No',
	5. A6: 'No',
	6. A8: 'No',
	7. A9: 'No'
	8. }</pre>
			<pre>1. {
			2. "response": true,
			3. "code": 200,
			4. "response_cluster": "1",
			5. "score_percentage": "0",
			6. "insight": "Not compliant in SaaS – Identity Management Operations related controls. Critical risk of security incidents related to the operations side of the identity management controls within SaaS application. Considerable effort is required to improve compliance to Identity Management Operations controls.",
			7. "recommendation": "Highly recommend referring to Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public</pre>
				Yes

		<pre>cloud services - 3.A - Assessing the SaaS cloud Identity Management section, following the proposed 5 step subprocess, and going through the process annually."
		}</pre>	

Category A – Ops/ Scenario 3	<pre>{
	A1: 'Yes',
	A2: 'Yes',
	A5: 'Yes',
	A6: 'No',
	A8: 'Yes',
	A9: 'Yes'
	}</pre>
		<pre>{
		"response": true,
		"code": 200,
		"response_cluster": "0",
		"score_percentage": "100",
		"insight": "Compliant in SaaS - Identity Management Operations related controls. Low risk of security incidents related to the operations side of the identity management controls within SaaS application.",
		"recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3.A - Assessing the SaaS cloud Identity Management section, following the proposed 5 step subprocess, and going through the process annually."
		}</pre>
			Yes

Category A – Ops/ Scenario 4	<pre>{
	A1: 'No',
	A2: 'No',
	A5: 'No',
	A6: 'Yes',
	A8: 'No',
	A9: 'No'
	}</pre>
		<pre>{
		"response": true,
		"code": 200,
		"response_cluster": "1",
		"score_percentage": "0",
		"insight": "Not compliant in SaaS – Identity Management Operations related controls. Critical risk of security incidents related to the operations side of the identity management controls within SaaS application. Considerable effort is required to improve compliance to Identity Management Operations controls.",
		"recommendation": "Highly recommend referring to Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3.A - Assessing the SaaS cloud Identity Management section, following the proposed 5 step subprocess, and going through the process annually."
		}</pre>
			Yes

Category A – Ops/ Scenario 5	<pre>{
	A1: 'Yes',
	A2: 'Yes',
	A5: 'Yes',
	A6: 'N/A',
	A8: 'Yes',
	A9: 'Yes'
	}</pre>
		<pre>{
		"response": true,
		"code": 200,
		"response_cluster": "0",
		"score_percentage": "100",
		"insight": "Compliant in SaaS - Identity Management Operations related</pre>
			Yes

			<pre>controls. Low risk of security incidents related to the operations side of the identity management controls within SaaS application.",
			7. "recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3.A - Assessing the SaaS cloud Identity Management section, following the proposed 5 step subprocess, and going through the process annually."
			8. }</pre>	

Category A – Ops/ Scenario 6	<pre>1. {
	2. A1: 'No',
	3. A2: 'No',
	4. A5: 'No',
	5. A6: 'N/A',
	6. A8: 'No',
	7. A9: 'No'
	8. }</pre>
			<pre>1. {
			2. "response": true,
			3. "code": 200,
			4. "response_cluster": "1",
			5. "score_percentage": "0",
			6. "insight": "Not compliant in SaaS – Identity Management Operations related controls. Critical risk of security incidents related to the operations side of the identity management controls within SaaS application. Considerable effort is required to improve compliance to Identity Management Operations controls.",
			7. "recommendation": "Highly recommend referring to Enhanced Cloud Security and</pre>
				Yes

			<pre>Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3.A - Assessing the SaaS cloud Identity Management section, following the proposed 5 step subprocess, and going through the process annually."
			}</pre>	

Category A – Ops/ Scenario 7	<pre>{
	A1: 'Yes',
	A2: 'Yes',
	A5: 'No',
	A6: 'N/A',
	A8: 'No',
	A9: 'No'
	}</pre>
			<pre>{
			"response": true,
			"code": 200,
			"response_cluster": "2",
			"score_percentage": "40",
			"insight": "Not compliant with mandatory controls required in the SaaS - Identity Management Operations section and complete lack compliance. Medium to high risk of security incidents related to the operations side of the identity management controls within SaaS application. There is room for improvement in the Identity Management Operations side to better compliance and security.",
			"recommendation": "Recommend referring Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3.A - Assessing the SaaS cloud Identity Management section, following the proposed 5 step</pre>
				Yes

		<pre>subprocess, and going through the process annually."
		}</pre>	

Category B – Gov/ Scenario 1	<pre>{
	B3: 'Yes',
	B4: 'Yes',
	B5: 'Yes',
	B6: 'Yes',
	B7: 'Yes',
	B8: 'Yes',
	B11: 'Yes',
	B13: 'Yes',
	B14: 'Yes',
	B15: 'Yes',
	B17: 'Yes',
	B21: 'Yes',
	B22: 'Yes',
	B23: 'Yes',
	B24: 'Yes',
	B25: 'Yes'
	}</pre>
		<pre>{
		"response": true,
		"code": 200,
		"response_cluster": "0",
		"score_percentage": "100",
		"insight": "Compliant in SaaS - Metastructure Governance related controls. Low risk of security incidents related to the governance side of the metastructure controls within SaaS application.",
		"recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. B - Assessing the SaaS cloud Metastructure section, following the proposed 5 step subprocess, and going through the process annually."
		}</pre>
			Yes

Category B – Gov/ Scenario 2	<pre>{
	B3: 'No',
	B4: 'No',
	B5: 'No',
	B6: 'No',
	B7: 'No',
	B8: 'No',
	B11: 'No',
	B13: 'No',
	B14: 'No',</pre>
		<pre>{
		"response": true,
		"code": 200,
		"response_cluster": "1",
		"score_percentage": "0",
		"insight": "Not compliant in SaaS – Metastructure Governance related controls. Critical/ high risk of</pre>
			Yes

	<pre>11. B15: 'No',
	12. B17: 'No',
	13. B21: 'No',
	14. B22: 'No',
	15. B23: 'No',
	16. B24: 'No',
	17. B25: 'No'
	18. }</pre>
		<pre>security incidents related to the operations side of the metastructure controls within SaaS application. Considerable effort is required to improve compliance with Metastructure Operations controls.",
		7. "recommendation": "Highly recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. B - Assessing the SaaS cloud Metastructure section, following the proposed 5 step subprocess, and going through the process annually."
		8. }</pre>	

Category B – Gov/ Scenario 3	<pre>1. {
	2. B3: 'Yes',
	3. B4: 'Yes',
	4. B5: 'Yes',
	5. B6: 'Yes',
	6. B7: 'Yes',
	7. B8: 'No',
	8. B11: 'Yes',
	9. B13: 'Yes',
	10. B14: 'Yes',
	11. B15: 'Yes',
	12. B17: 'Yes',
	13. B21: 'Yes',
	14. B22: 'Yes',
	15. B23: 'Yes',
	16. B24: 'Yes',
	17. B25: 'Yes'
	18. }</pre>
		<pre>1. {
		2. "response": true,
		3. "code": 200,
		4. "response_cluster": "0",
		5. "score_percentage": "100",
		6. "insight": "Compliant in SaaS - Metastructure Governance related controls. Low risk of security incidents related to the governance side of the metastructure controls within SaaS application.",
		7. "recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public</pre>
			Yes

		<pre>cloud services - 3. B - Assessing the SaaS cloud Metastructure section, following the proposed 5 step subprocess, and going through the process annually."
		}</pre>	

Category B – Gov/ Scenario 4	<pre>{
	B3: 'No',
	B4: 'No',
	B5: 'No',
	B6: 'No',
	B7: 'No',
	B8: 'Yes',
	B11: 'No',
	B13: 'No',
	B14: 'No',
	B15: 'No',
	B17: 'No',
	B21: 'No',
	B22: 'No',
	B23: 'No',
	B24: 'No',
	B25: 'No'
	}</pre>
		<pre>{
		"response": true,
		"code": 200,
		"response_cluster": "1",
		"score_percentage": "0",
		"insight": "Not compliant in SaaS – Metastructure Governance related controls. Critical/ high risk of security incidents related to the operations side of the metastructure controls within SaaS application. Considerable effort is required to improve compliance with Metastructure Operations controls.",
		"recommendation": "Highly recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. B - Assessing the SaaS cloud Metastructure section, following the proposed 5 step subprocess, and going through the process annually."
		}</pre>
			Yes

Category B – Gov/ Scenario 5		<pre>{
		  B3: 'Yes',
		  B4: 'Yes',
		  B5: 'Yes',
		  B6: 'Yes',
		  B7: 'Yes',
		  B8: 'N/A',
		  B11: 'Yes',
		  B13: 'Yes',
		  B14: 'Yes',
		  B15: 'Yes',
		  B17: 'Yes',
		  B21: 'Yes',
		  B22: 'Yes',
		  B23: 'Yes',
		  B24: 'Yes',
		  B25: 'Yes'
		}</pre>
				<pre>{
				  "response": true,
				  "code": 200,
				  "response_cluster": "0",
				  "score_percentage": "100",
				  "insight": "Compliant in SaaS - Metastructure Governance related controls. Low risk of security incidents related to the governance side of the metastructure controls within SaaS application.",
				  "recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. B - Assessing the SaaS cloud Metastructure section, following the proposed 5 step subprocess, and going through the process annually."
				}</pre>
					Yes

Category B – Gov/ Scenario 6		<pre>{
		  B3: 'No',
		  B4: 'No',
		  B5: 'No',
		  B6: 'No',
		  B7: 'No',
		  B8: 'N/A',
		  B11: 'No',
		  B13: 'No',
		  B14: 'No',
		  B15: 'No',
		  B17: 'No',
		  B21: 'No',
		  B22: 'No',
		  B23: 'No',</pre>
				<pre>{
				  "response": true,
				  "code": 200,
				  "response_cluster": "1",
				  "score_percentage": "0",
				  "insight": "Not compliant in SaaS – Metastructure Governance related controls. Critical/ high risk of security incidents related to the operations side of the metastructure controls within SaaS application. Considerable effort is</pre>
					Yes

		16. B24: 'No', 17. B25: 'No' 18. }		required to improve compliance with Metastructure Operations controls.", 7. "recommendation": "Highly recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. B - Assessing the SaaS cloud Metastructure section, following the proposed 5 step subprocess, and going through the process annually." 8. }	
Category B – Gov/ Scenario 7		1. { 2. B3: 'Yes', 3. B4: 'Yes', 4. B5: 'No', 5. B6: 'No', 6. B7: 'Yes', 7. B8: 'N/A', 8. B11: 'Yes', 9. B13: 'No', 10. B14: 'Yes', 11. B15: 'No', 12. B17: 'Yes', 13. B21: 'Yes', 14. B22: 'No', 15. B23: 'No', 16. B24: 'No', 17. B25: 'No' 18. }		1. { 2. "response": true, 3. "code": 200, 4. "response_cluster": "2", 5. "score_percentage": "47", 6. "insight": "Not compliant in SaaS – Metastructure Governance related controls. Critical/ high risk of security incidents related to the operations side of the metastructure controls within SaaS application. Considerable effort is required to improve compliance with Metastructure Operations controls.", 7. "recommendation": "Highly recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud	Yes

			<pre>Systems consuming public cloud services - 3. B - Assessing the SaaS cloud Metastructure section, following the proposed 5 step subprocess, and going through the process annually."
			}</pre>	

Category B – Ops/ Scenario 1	<pre>{
	B1: 'Yes',
	B2: 'Yes',
	B9: 'Yes',
	B10: 'Yes',
	B12: 'Yes',
	B16: 'Yes',
	B18: 'Yes',
	B19: 'Yes',
	B20: 'Yes'
	}</pre>
			<pre>{
			"response": true,
			"code": 200,
			"response_cluster": "0",
			"score_percentage": "100",
			"insight": "Compliant in SaaS - Metastructure Operations related controls. Low risk of security incidents related to the operations side of the metastructure within SaaS application.",
			"recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. B - Assessing the SaaS cloud Metastructure section, following the proposed 5 step subprocess, and going through the process annually."
			}</pre>
				Yes

Category B – Ops/ Scenario 2	<pre>{
	B1: 'No',
	B2: 'No',
	B9: 'No',
	B10: 'No',</pre>
			<pre>{
			"response": true,
			"code": 200,
			"response_cluster": "1",
			"score_percentage": "0",</pre>
				Yes

		6. B12: 'No', 7. B16: 'No', 8. B18: 'No', 9. B19: 'No', 10. B20: 'No' 11. }		6. "insight": "Not compliant in SaaS – Metastructure Operations related controls. Critical risk of security incidents related to the operations side of the metastructure controls within SaaS application. Considerable effort is required to improve compliance with Metastructure Operations controls.", 7. "recommendation": "Highly recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. B - Assessing the SaaS cloud Metastructure section, following the proposed 5 step subprocess, and going through the process annually." 8. }	
Category B – Ops/ Scenario 3		1. { 2. B1: 'No', 3. B2: 'No', 4. B9: 'Yes', 5. B10: 'Yes', 6. B12: 'Yes', 7. B16: 'Yes', 8. B18: 'No', 9. B19: 'Yes', 10. B20: 'Yes' 11. }		1. { 2. "response": true, 3. "code": 200, 4. "response_cluster": "0", 5. "score_percentage": "100", 6. "insight": "Compliant in SaaS - Metastructure Operations related controls. Low risk of security incidents related to the operations side of the metastructure within SaaS application.", 7. "recommendation": "Recommend referring to the Enhanced Cloud	Yes

			<pre>Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. B - Assessing the SaaS cloud Metastructure section, following the proposed 5 step subprocess, and going through the process annually."
			}</pre>	

Category B – Ops/ Scenario 4	<pre>{
	B1: 'Yes',
	B2: 'Yes',
	B9: 'No',
	B10: 'No',
	B12: 'No',
	B16: 'No',
	B18: 'Yes',
	B19: 'No',
	B20: 'No'
	}</pre>
			<pre>{
			"response": true,
			"code": 200,
			"response_cluster": "1",
			"score_percentage": "0",
			"insight": "Not compliant in SaaS – Metastructure Operations related controls. Critical risk of security incidents related to the operations side of the metastructure controls within SaaS application. Considerable effort is required to improve compliance with Metastructure Operations controls.",
			"recommendation": "Highly recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. B - Assessing the SaaS cloud Metastructure section, following the proposed 5 step subprocess, and going through the process annually."</pre>
				Yes

		<pre>8. }</pre>	

Category B – Ops/ Scenario 5	<pre>1. {
	2. B1: 'N/A',
	3. B2: 'N/A',
	4. B9: 'Yes',
	5. B10: 'Yes',
	6. B12: 'Yes',
	7. B16: 'Yes',
	8. B18: 'N/A',
	9. B19: 'Yes',
	10. B20: 'Yes'
	11. }</pre>
		<pre>1. {
		2. "response": true,
		3. "code": 200,
		4. "response_cluster": "0",
		5. "score_percentage": "100",
		6. "insight": "Compliant in SaaS - Metastructure Operations related controls. Low risk of security incidents related to the operations side of the metastructure within SaaS application.",
		7. "recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. B - Assessing the SaaS cloud Metastructure section, following the proposed 5 step subprocess, and going through the process annually."
		8. }</pre>
			Yes

Category B – Ops/ Scenario 6	<pre>1. {
	2. B1: 'N/A',
	3. B2: 'N/A',
	4. B9: 'No',
	5. B10: 'No',
	6. B12: 'No',
	7. B16: 'No',
	8. B18: 'N/A',
	9. B19: 'No',
	10. B20: 'No'
	11. }</pre>
		<pre>1. {
		2. "response": true,
		3. "code": 200,
		4. "response_cluster": "2",
		5. "score_percentage": "0",
		6. "insight": "Not compliant in SaaS – Metastructure Operations related controls. Critical risk of security incidents related to the operations side of the metastructure controls within SaaS</pre>
			Yes

			<pre>application. Considerable effort is required to improve compliance with Metastructure Operations controls.",
			7. "recommendation": "Highly recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. B - Assessing the SaaS cloud Metastructure section, following the proposed 5 step subprocess, and going through the process annually."
			8. }</pre>	

Category B – Ops/ Scenario 7	<pre>1. { B1: 'N/A',
	2. B2: 'N/A',
	3. B9: 'Yes',
	4. B10: 'Yes',
	5. B12: 'No',
	6. B16: 'Yes',
	7. B18: 'N/A',
	8. B19: 'No',
	9. B20: 'No'
	10. }</pre>
			<pre>1. {
			2. "response": true,
			3. "code": 200,
			4. "response_cluster": "2",
			5. "score_percentage": "50",
			6. "insight": "Not compliant in SaaS – Metastructure Operations related controls. Critical risk of security incidents related to the operations side of the metastructure controls within SaaS application. Considerable effort is required to improve compliance with Metastructure Operations controls.",
			7. "recommendation": "Highly recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud</pre>
				Yes

		<pre>Systems consuming public cloud services - 3. B - Assessing the SaaS cloud Metastructure section, following the proposed 5 step subprocess, and going through the process annually."
		}</pre>	

Category C – Gov/ Scenario 1	<pre>{
	C3: 'Yes',
	C4: 'Yes',
	C5: 'Yes',
	C8: 'Yes',
	C9: 'Yes',
	C10: 'Yes'
	}</pre>
		<pre>{
		"response": true,
		"code": 200,
		"response_cluster": "0",
		"score_percentage": "100",
		"insight": "Compliant in SaaS - Applistructure & Infostructure Governance related controls. Low risk of security incidents related to the governance side of the Applistructure & Infostructure controls within SaaS application.",
		"recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. C - Assessing the SaaS cloud Applistructure & Infostructure section, following the proposed 5 step subprocess, and going through the process annually."
		}</pre>
			Yes

Category C – Gov/ Scenario 2	<pre>{
	  C3: 'No',
	  C4: 'No',
	  C5: 'No',
	  C8: 'No',
	  C9: 'No',
	  C10: 'No'
	}</pre>
		<pre>{
		  "response": true,
		  "code": 200,
		  "response_cluster": "1",
		  "score_percentage": "0",
		  "insight": "Not compliant in SaaS – Applistructure & Infostructure Governance related controls. Critical risk of security incidents related to your SaaS application's Applistructure & Infostructure area. Considerable effort is required to improve compliance to Applistructure & Infostructure Governance controls.",
		  "recommendation": "Highly recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. C - Assessing the SaaS cloud Applistructure & Infostructure section, following the proposed 5 step subprocess, and going through the process annually."
		}</pre>
			Yes

Category C – Gov/ Scenario 3	<pre>{
	  C3: 'Yes',
	  C4: 'Yes',
	  C5: 'No',
	  C8: 'Yes',
	  C9: 'Yes',
	  C10: 'Yes'</pre>
		<pre>{
		  "response": true,
		  "code": 200,
		  "response_cluster": "0",
		  "score_percentage": "100",</pre>
			Yes

	<pre>8. }</pre>		<pre>6. "insight": "Compliant in SaaS - Applistructure & Infostructure Governance related controls. Low risk of security incidents related to the governance side of the Applistructure & Infostructure controls within SaaS application.",
			7. "recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. C - Assessing the SaaS cloud Applistructure & Infostructure section, following the proposed 5 step subprocess, and going through the process annually."
			8. }</pre>	

Category C – Gov/ Scenario 4	<pre>1. {
	2. C3: 'No',
	3. C4: 'No',
	4. C5: 'Yes',
	5. C8: 'No',
	6. C9: 'No',
	7. C10: 'No'
	8. }</pre>
			<pre>1. {
			2. "response": true,
			3. "code": 200,
			4. "response_cluster": "1",
			5. "score_percentage": "0",
			6. "insight": "Not compliant in SaaS – Applistructure & Infostructure Governance related controls. Critical risk of security incidents related to your SaaS application's Applistructure & Infostructure area. Considerable effort is required to improve compliance to Applistructure &</pre>
				Yes

			<pre>Infostructure Governance controls.",
			7. "recommendation": "Highly recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. C - Assessing the SaaS cloud Applistructure & Infostructure section, following the proposed 5 step subprocess, and going through the process annually."
			8. }</pre>	

Category C – Gov/ Scenario 5	<pre>1. {
	2. C3: 'Yes',
	3. C4: 'Yes',
	4. C5: 'N/A',
	5. C8: 'Yes',
	6. C9: 'Yes',
	7. C10: 'Yes'
	8. }</pre>
			<pre>1. {
			2. "response": true,
			3. "code": 200,
			4. "response_cluster": "0",
			5. "score_percentage": "100",
			6. "insight": "Compliant in SaaS - Applistructure & Infostructure Governance related controls. Low risk of security incidents related to the governance side of the Applistructure & Infostructure controls within SaaS application.",
			7. "recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. C - Assessing the SaaS cloud Applistructure & Infostructure section, following the proposed 5</pre>
				Yes

		<pre>step subprocess, and going through the process annually."
		}</pre>	

Category C – Gov/ Scenario 6	<pre>{
	C3: 'No',
	C4: 'No',
	C5: 'N/A',
	C8: 'No',
	C9: 'No',
	C10: 'No'
	}</pre>
		<pre>{
		"response": true,
		"code": 200,
		"response_cluster": "1",
		"score_percentage": "0",
		"insight": "Not compliant in SaaS – Applistructure & Infostructure Governance related controls. Critical risk of security incidents related to your SaaS application's Applistructure & Infostructure area. Considerable effort is required to improve compliance to Applistructure & Infostructure Governance controls.",
		"recommendation": "Highly recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. C - Assessing the SaaS cloud Applistructure & Infostructure section, following the proposed 5 step subprocess, and going through the process annually."
		}</pre>
			Yes

Category C – Gov/ Scenario 7		<pre>{
		  C3: 'No',
		  C4: 'No',
		  C5: 'N/A',
		  C8: 'Yes',
		  C9: 'Yes',
		  C10: 'No'
		}</pre>
				<pre>{
				  "response": true,
				  "code": 200,
				  "response_cluster": "2",
				  "score_percentage": "40",
				  "insight": "Not compliant with mandatory controls required in the SaaS - Applistructure & Infostructure Governance section and complete lack compliance. Medium to high risk of security incidents related to the governance side of the Applistructure & Infostructure controls within SaaS application. There is room for improvement in the Applistructure & Infostructure Governance side to better compliance and security.",
				  "recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. C - Assessing the SaaS cloud Applistructure & Infostructure section, following the proposed 5 step subprocess, and going through the process annually."
				}</pre>
					Yes

Category C – Ops/ Scenario 1		<pre>{
		  C1: 'Yes',
		  C2: 'Yes',
		  C6: 'Yes',</pre>
				<pre>{
				  "response": true,
				  "code": 200,
				  "response_cluster": "0",</pre>
					Yes

	<pre>5. C7: 'Yes'
	6. }</pre>
			<pre>5. "score_percentage": "100",
			6. "insight": "Compliant in SaaS - Applistructure & Infostructure Operations related controls. Low risk of security incidents related to the operations side of the Applistructure & Infostructure controls within SaaS application.",
			7. "recommendation": "Recommend referring to Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. C - Assessing the SaaS cloud Applistructure & Infostructure section, following the proposed 5 step subprocess, and going through the process annually."
			8. }</pre>	

Category C – Ops/ Scenario 2	<pre>1. {
	2. C1: 'No',
	3. C2: 'No',
	4. C6: 'No',
	5. C7: 'No'
	6. }</pre>
			<pre>1. {
			2. "response": true,
			3. "code": 200,
			4. "response_cluster": "1",
			5. "score_percentage": "0",
			6. "insight": "Not compliant in SaaS – Applistructure & Infostructure Operations related controls. Critical risk of security incidents related to your SaaS application's Applistructure & Infostructure area. Considerable effort is required to improve compliance to Applistructure &</pre>
				Yes

			<pre>Infostructure Operations controls.",
			7. "recommendation": "Highly recommend referring to Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. C - Assessing the SaaS cloud Applistructure & Infostructure section, following the proposed 5 step subprocess, and going through the process annually."
			8. }</pre>	

Category C - Ops/ Scenario 7	<pre>1. {
	2. C1: 'No',
	3. C2: 'No',
	4. C6: 'Yes',
	5. C7: 'Yes'
	6. }</pre>
			<pre>1. {
			2. "response": true,
			3. "code": 200,
			4. "response_cluster": "4",
			5. "score_percentage": "50",
			6. "insight": "Not compliant with mandatory controls required in the SaaS - Applistructure & Infostructure Operations section and complete lack compliance. Medium to high risk of security incidents related to the operations side of the Applistructure & Infostructure controls within SaaS application. There is room for improvement in the Applistructure & Infostructure Operations side to better compliance and security.",
			7. "recommendation": "Recommend referring to Enhanced Cloud Security</pre>
				Yes

		and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. C - Assessing the SaaS cloud Applistructure & Infostructure section, following the proposed 5 step subprocess, and going through the process annually." 8. }	
Category D – Gov/ Scenario 1	1. { 2. D2: 'Yes', 3. D7: 'Yes' 4. }	1. { 2. "response": true, 3. "code": 200, 4. "response_cluster": "2", 5. "score_percentage": "100", 6. "insight": "Compliant in SaaS - Infrastructure Governance related controls. Low risk of security incidents related to the governance side of the infrastructure controls within SaaS application.", 7. "recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. D - Assessing the SaaS cloud Infrastructure section, following the proposed 5 step subprocess, and going through the process annually." 8. }	Yes

Category D – Gov/ Scenario 2	<pre>{
	  D2: 'No',
	  D7: 'No'
	}</pre>
		<pre>{
		  "response": true,
		  "code": 200,
		  "response_cluster": "3",
		  "score_percentage": "0",
		  "insight": "Not compliant in SaaS – Infrastructure Governance related controls. Critical risk of security incidents related to the Infrastructure area of your SaaS application. Considerable effort is required to improve compliance to Infrastructure Governance controls.",
		  "recommendation": "Highly recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. D - Assessing the SaaS cloud Infrastructure section, following the proposed 5 step subprocess, and going through the process annually."
		}</pre>
			Yes

Category D – Gov/ Scenario 7	<pre>{
	  D2: 'Yes',
	  D7: 'No'
	}</pre>
		<pre>{
		  "response": true,
		  "code": 200,
		  "response_cluster": "1",
		  "score_percentage": "50",
		  "insight": "Not compliant with mandatory controls required in the SaaS - Infrastructure Governance section and</pre>
			Yes

			<pre>lack complete compliance. Medium to high risk of security incidents related to the governance side of the Infrastructure controls within SaaS application. There is room for improvement in the Infrastructure Governance side to better compliance and security.",
			"recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. D - Assessing the SaaS cloud Infrastructure section, following the proposed 5 step subprocess, and going through the process annually."
			}</pre>	

Category D – Ops/ Scenario 1	<pre>{
	D1: 'Yes',
	D3: 'Yes',
	D4: 'Yes',
	D5: 'Yes',
	D6: 'Yes',
	D8: 'Yes',
	D9: 'Yes'
	}</pre>
			<pre>{
			"response": true,
			"code": 200,
			"response_cluster": "0",
			"score_percentage": "100",
			"insight": "Compliant in SaaS - Infrastructure Operations related controls. Low risk of security incidents related to the operations side of the infrastructure controls within SaaS application.",
			"recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance</pre>
				Yes

			<pre>Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. D - Assessing the SaaS cloud Infrastructure section, following the proposed 5 step subprocess, and going through the process annually."
			}</pre>	

Category D – Ops/ Scenario 2	<pre>{
	D1: 'No',
	D3: 'No',
	D4: 'No',
	D5: 'No',
	D6: 'No',
	D8: 'No',
	D9: 'No'
	}</pre>
			<pre>{
			"response": true,
			"code": 200,
			"response_cluster": "1",
			"score_percentage": "0",
			"insight": "Not compliant in SaaS – Infrastructure operations related controls. Critical risk of security incidents related to the Infrastructure area of your SaaS application. Considerable effort is required to improve compliance to Infrastructure Operations controls.",
			"recommendation": "Highly recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. D - Assessing the SaaS cloud Infrastructure section, following the proposed 5 step subprocess, and going through the process annually."</pre>
				Yes

		<pre>8. }</pre>	

Category D – Ops/ Scenario 3	<pre>1. {
	2. D1: 'Yes',
	3. D3: 'Yes',
	4. D4: 'Yes',
	5. D5: 'No',
	6. D6: 'Yes',
	7. D8: 'Yes',
	8. D9: 'Yes'
	9. }</pre>
		<pre>1. {
		2. "response": true,
		3. "code": 200,
		4. "response_cluster": "0",
		5. "score_percentage": "100",
		6. "insight": "Compliant in SaaS - Infrastructure Operations related controls. Low risk of security incidents related to the operations side of the infrastructure controls within SaaS application.",
		7. "recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. D - Assessing the SaaS cloud Infrastructure section, following the proposed 5 step subprocess, and going through the process annually."
		8. }</pre>
			Yes

Category D – Ops/ Scenario 4	<pre>1. {
	2. D1: 'No',
	3. D3: 'No',
	4. D4: 'No',
	5. D5: 'Yes',
	6. D6: 'No',
	7. D8: 'No',
	8. D9: 'No'
	9. }</pre>
		<pre>1. {
		2. "response": true,
		3. "code": 200,
		4. "response_cluster": "1",
		5. "score_percentage": "0",
		6. "insight": "Not compliant in SaaS – Infrastructure operations related controls. Critical risk of security incidents related to the Infrastructure area of</pre>
			Yes

			<pre>your SaaS application. Considerable effort is required to improve compliance to Infrastructure Operations controls.",
			7. "recommendation": "Highly recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. D - Assessing the SaaS cloud Infrastructure section, following the proposed 5 step subprocess, and going through the process annually."
			8. }</pre>	

Category D – Ops/ Scenario 5	<pre>1. {
	2. D1: 'Yes',
	3. D3: 'Yes',
	4. D4: 'Yes',
	5. D5: 'N/A',
	6. D6: 'Yes',
	7. D8: 'Yes',
	8. D9: 'Yes'
	9. }</pre>
			<pre>1. {
			2. "response": true,
			3. "code": 200,
			4. "response_cluster": "0",
			5. "score_percentage": "100",
			6. "insight": "Compliant in SaaS - Infrastructure Operations related controls. Low risk of security incidents related to the operations side of the infrastructure controls within SaaS application.",
			7. "recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. D - Assessing the SaaS cloud</pre>
				Yes

		<pre>Infrastructure section, following the proposed 5 step subprocess, and going through the process annually."
		}</pre>	

Category D – Ops/ Scenario 6	<pre>{
	D1: 'No',
	D3: 'No',
	D4: 'No',
	D5: 'N/A',
	D6: 'No',
	D8: 'No',
	D9: 'No'
	}</pre>
		<pre>{
		"response": true,
		"code": 200,
		"response_cluster": "1",
		"score_percentage": "0",
		"insight": "Not compliant in SaaS – Infrastructure operations related controls. Critical risk of security incidents related to the Infrastructure area of your SaaS application. Considerable effort is required to improve compliance to Infrastructure Operations controls.",
		"recommendation": "Highly recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. D - Assessing the SaaS cloud Infrastructure section, following the proposed 5 step subprocess, and going through the process annually."
		}</pre>
			Yes

Category D – Ops/ Scenario 7	<pre>{
	D1: 'No',
	D3: 'No',
	D4: 'Yes',</pre>
		<pre>{
		"response": true,
		"code": 200,
		"response_cluster": "2",</pre>
			Yes

	5. D5: 'N/A', 6. D6: 'Yes', 7. D8: 'No', 8. D9: 'Yes' 9. }	5. "score_percentage": "50", 6. "insight": "Not compliant with mandatory controls required in the SaaS - Infrastructure Operations section and complete lack compliance. Medium to high risk of security incidents related to the operations side of the Infrastructure controls within SaaS application. There is room for improvement in the Infrastructure Operations side to better compliance and security.", 7. "recommendation": "Recommend referring to the Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services - 3. D - Assessing the SaaS cloud Infrastructure section, following the proposed 5 step subprocess, and going through the process annually." 8. }	

All the test scenarios covered yielded the expected outcomes. When we take test scenarios 1 – 6 for each category into account, the respective model for that category was able to predict the expected cluster all the time, which makes the accuracy of the machine learning model 100% for those scenarios. In all those scenarios, cluster prediction belonged to either Type 1 or Type 2 based on the cluster interpretations discussed under section 4.1.6.3. For scenario 7, all the models except the Category B – Governance (Cat B - Gov) and Category B – Operations (Cat B – Ops) belonged to the cluster interpretation of Type 3. Both Cat B – Gov and Cat B – Ops didn't include any cluster interpretations belonging to Type 3.

Since cluster interpretation was a manual process, it was mainly based on intuition by observing the cluster predictions on the training data set. I had to interpret different clusters predicted by the machine learning models under a single interpretation in this process as the feature data observations under each cluster and their interpretations were similar. This is often a problem in real-world data sets like the ones we have used to train the models within this implementation [56] . It's also a critical observation of the machine learning model implementation.

The above observation was visible when deciding the optimum number of clusters per category. Several attempts were made to find the optimal number of clusters using the elbow method for machine learning models of each category. Sometimes, this led to similar data observations in different clusters and dissimilar data observations in the same cluster. The final optimal k value for each cluster was obtained only after several trial-and-error phases by decreasing and increasing the optimal value. In this trial-and-error phase, even reducing the optimum number of clusters even by one lead to having dissimilar data observations under the same cluster for several machine learning models (Cat A - Ops, Cat B - Ops, Cat C - Ops, Cat D - Gov, Cat D - Ops). So based on the use case of this implementation, having multiple clusters and interpreting them under a single type seemed to be a more logical approach rather than reducing the optimal cluster number. If we opted to proceed with a smaller number of clusters as the optimum number, the recommendations and insights based on cluster predictions could have gone meaningless as the same cluster includes dissimilar data observations.

This could be optimized by feeding more data into the clustering data set, which can be achieved by exposing the implemented services as a consumable product to end-users. Yet, it's still a critical observation that is visible when working with real-world data sets for building machine learning models.

5.2 – Survey result findings

This section presents the findings identified from the survey related to the process followed in section 4.1.1 – Data collection and organization. This includes survey result findings for sections 1 – 3. The main motive behind this was to gather information required for our training data set, which we discussed in detail in previous sections under implementation. The questions in sections 1 – 3 of the survey can be categorized as follows. All the questions are also available in Appendix B.

1) Intro Questionnaire
    - Identification of SaaS business type.
    - Identification of survey respondent's profile.
2) Assessing SaaS business domain
    - Identification of the business domain of the SaaS platform
    - Identification of the geographical locations and the regulatory compliance standard awareness of the SaaS business.
3) Assessing the Cloud Service Provider
    - Identification of the knowledge of the SaaS business around the shared responsibility model.
    - Identification of CSP products used by the respondents of the survey.

5.2.1 – Intro Questionnaire

This section focuses on identifying the SaaS business type of the survey respondents their respondents' profiles.

Based on the results shown in Figures 25 and 26, we can identify that a higher number of respondents of this survey were working within Startups and SMEs where the total employee count is between 0 – 15 and 15 – 50 respectively. So, we can conclude that the training data set used for training the machine learning model included the majority of the responses from employees working in emerging SaaS businesses, which was ideal for the purpose of this research.

Type of business

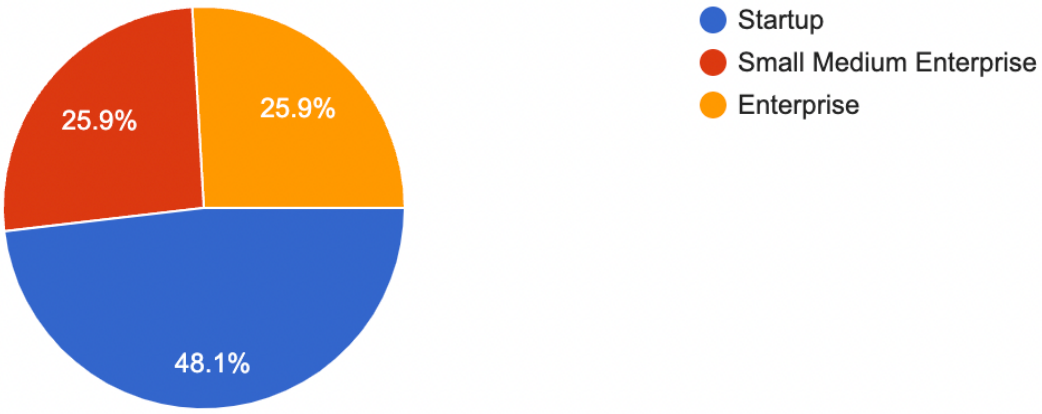


Figure 25 – Survey – Type of SaaS business

Number of employees

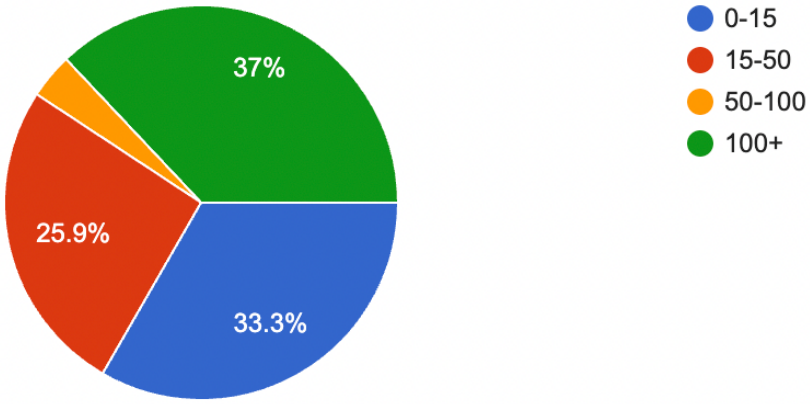


Figure 26 – Survey – Number of Employees

The results depicted in Figures 27 and 28 provide an insight into the respondents' individual profiles. Based on that we can see the job role distribution among many job roles related to the IT field while the majority of the respondent were either senior or higher level.

Your job area

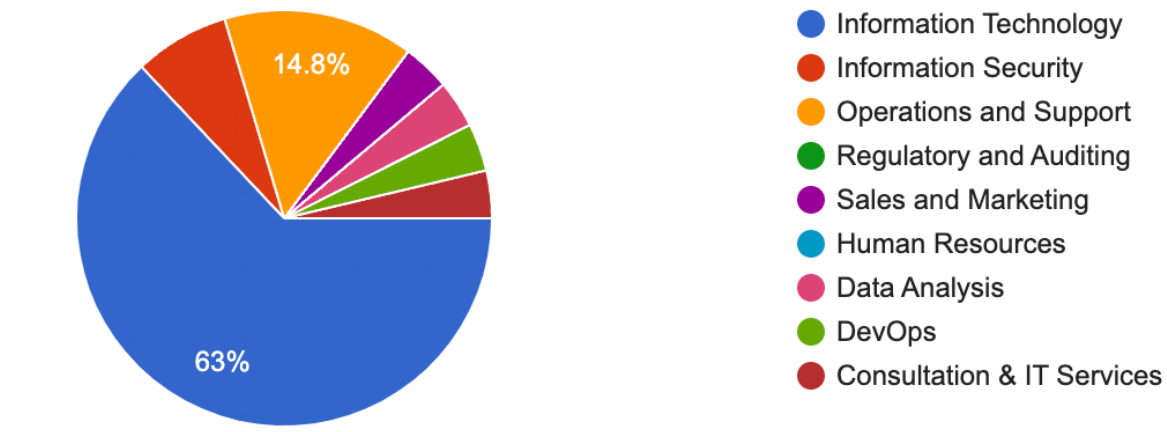


Figure 27 – Survey – Job area

Your job level

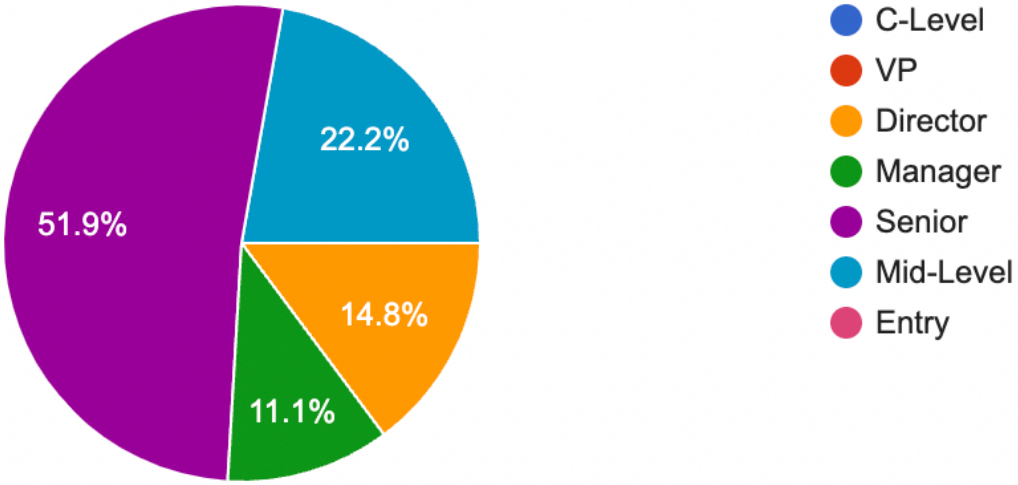


Figure 28 – Survey – Job levels

5.2.2 – Assessing SaaS Business Domain

This section captures data related to the business domain of the SaaS platform, the geographical location of the customer base, the awareness of the respondents on the regulatory and compliance standards applicable to the SaaS platform. The final result set showcase that the respondents are based on various SaaS business domains with their customers scattered across the globe.

What is the business domain of the SaaS business?

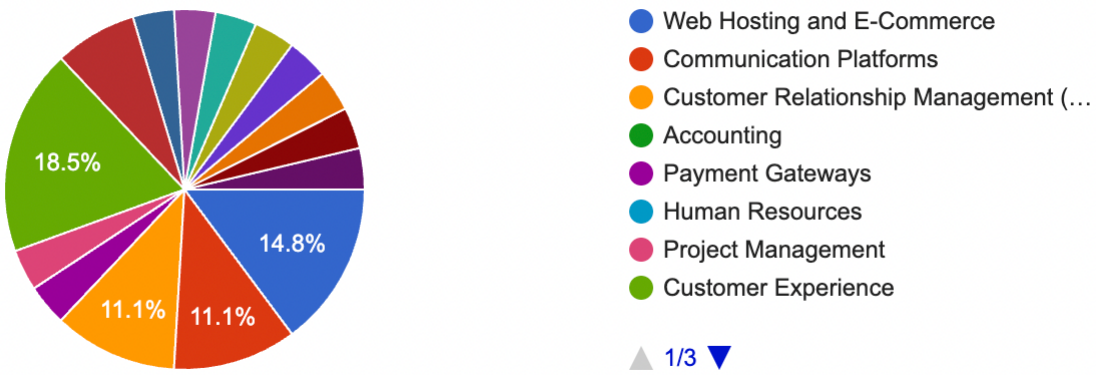


Figure 29 – Survey – SaaS business domains

What are the geographical locations of your targeted customer base?

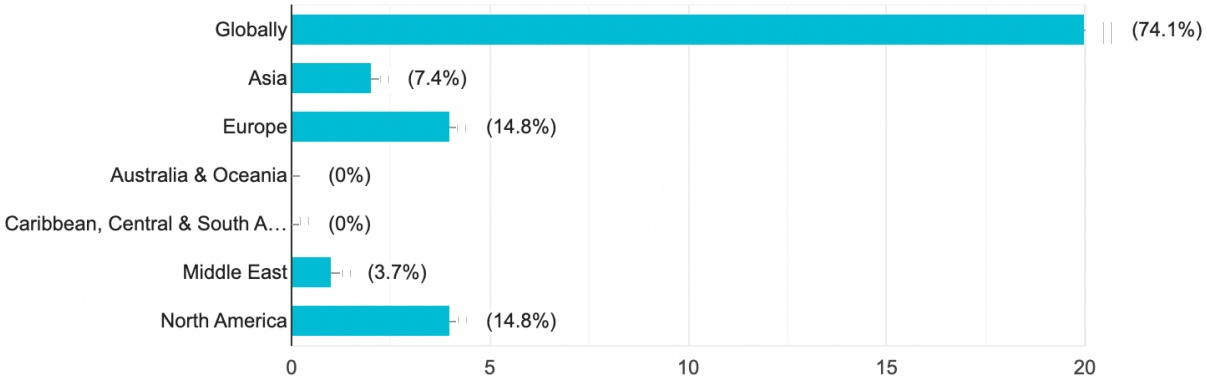


Figure 30 – Survey – Geographical locations of the customers

Are you aware of regulatory compliance standards applicable to your SaaS business?

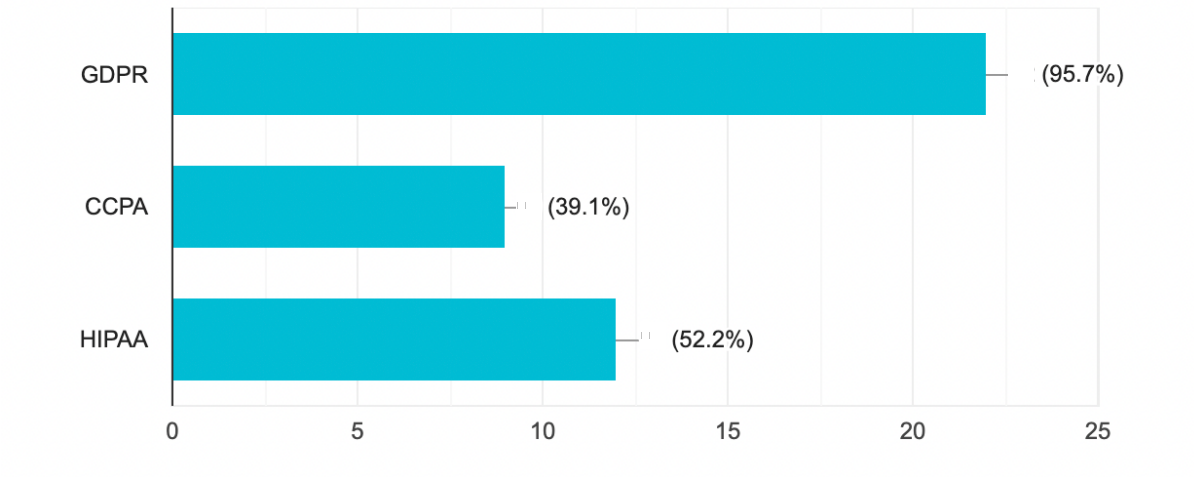


Figure 31 – Survey – Regulatory Compliance Standards Awareness

5.2.1 – Assessing the Cloud Service Provider

This section captures data related to the cloud deployment method used by the SaaS platform and whether the respondents are aware of the shared responsibility model between their cloud service provider and the SaaS platform. Based on the final result set, we can see that most respondents rely on the public cloud or a mix of public and private cloud and are aware of the shared responsibility model between cloud service consumers and cloud service providers.

What is the cloud deployment method/ model used by the SaaS platform?

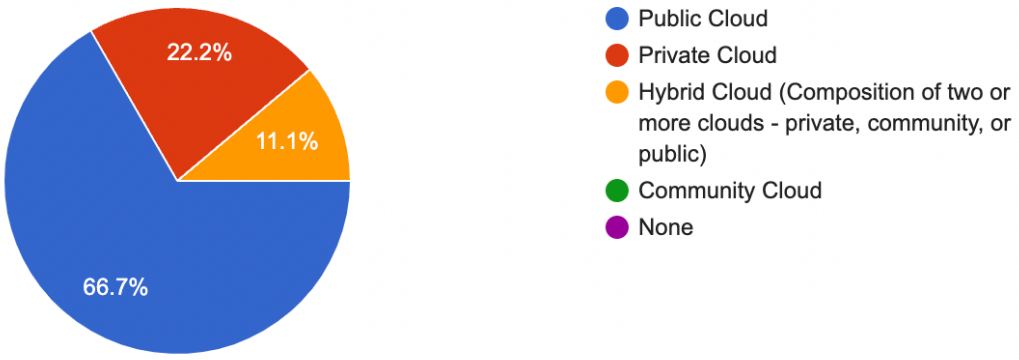


Figure 32 – Survey – Cloud deployment method used by the SaaS platform

What are the cloud service providers consumed by the SaaS platform?

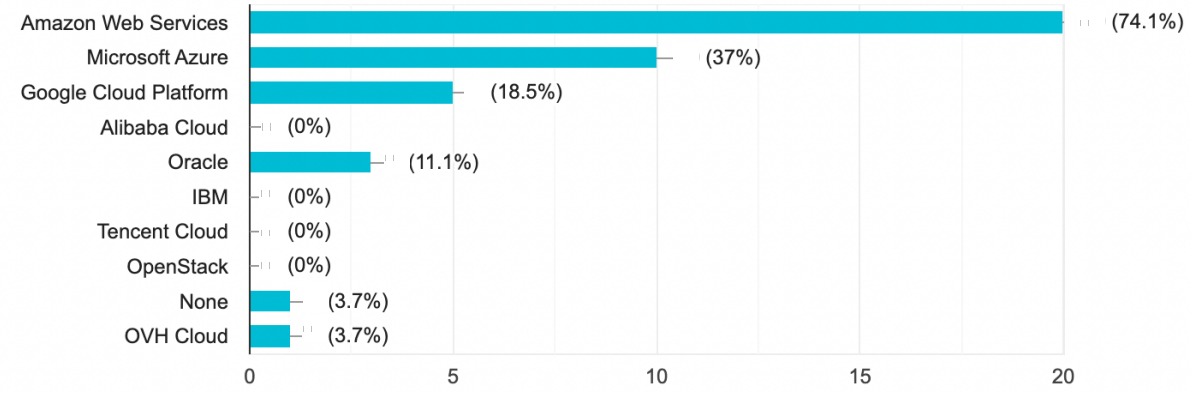


Figure 33 – Survey – CSP consumed by the SaaS platform

Do you evaluate and review the shared responsibility model of your cloud service provider and clearly understands which party is accountable (you and your cloud service provider) for security and compliance obligations?

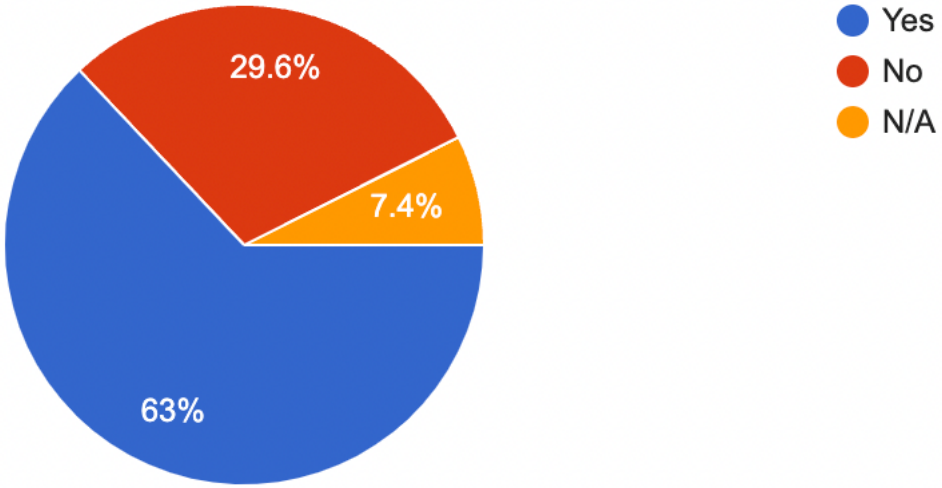


Figure 34 – Survey – Shared Responsibility Awareness

5.3 – Benchmark between existing cloud security models and proposed models

The benchmark process has been carried out to showcase how the proposed model and the approach used within that model are different to the existing ones. The existing models related to this domain were deeply studied within the Literature Review (Section 2.6). Some of the identified models were outdated and doesn't fit into the context that's covered in this research. The Cloud Multiple–Tenancy Model of NIST, Cloud Risks Accumulation Model and Jerico Fomu's Cloud Cube Model discussed within the research attempt carried out by Che *et al.* [45] were excluded due to that. All those three models extensively focus on cloud security threat identification. The Multiple-Tenancy Model of NIST is a model deeply focused on how multi-tenancy was handled within the cloud and security controls related to that. Jerico Fomu's Cloud Cube Model extensively discusses and focuses on security controls related to applications deployed both internally owned computing resources and other vendor-owned cloud computing resources. The Cloud Risk Accumulation model by CSA focuses on security controls related to different cloud services models (SaaS, PaaS and SaaS). The main idea for this model was based on the inherited relation between the service capability of different layers in cloud computing (IaaS is the foundation layer of all cloud services, PaaS is built upon IaaS and SaaS is built upon PaaS). Since the proposed reference model is focusing on emerging SaaS cloud systems consuming public cloud services, specifically focusing on all the security controls of building an Infrastructure as Services or a Platform as a Service is not required. Instead, the focus should be on the shared responsibility model as both public CSP and cloud consumers should be responsible for security within IaaS and PaaS services they use. None of the excluded models focused on the above-mentioned aspect either.

Based on the reviewed models, following models were chosen for benchmarking with the proposed reference model,

- The Mapping Model of Cloud Security and Compliance
- A Simple Cloud Security Process Model by CSA

Following factors were chosen as properties to assess in the benchmarking process. Benchmarking process identifies whether the assessed models are related to domains covered within this research attempt.

- **Ability to map cloud security threats and cloud regulatory compliance standards** – The model should enable its users the ability to map between cloud threats and cloud regulatory compliance standards.
- **Ability to assess cloud threats with cloud regulatory compliance standard goals** – The model should enable SaaS businesses to assess the work carried out in cloud threat identification and resolving with the cloud regulatory compliance standards goals specific for their business.
- **Adaptability** – The model should have the ability to evolve to future changes in cloud computing, cloud threats and cloud regulatory compliance standards domain.
- **Practicality and understandability** – The model should be practical to follow and implement with a clearly defined structure to deliver a better understanding to the end-user.
- **Uniqueness** – The model should have a unique focus on what type of cloud service models or delivery models that it's applicable. Becoming generic will increase the complexity of the model.
- **Coverage** – The model should cover all the aspects of the domains it is covering.

Table 26 – Benchmarking between proposed model and the reviewed models *(Spans across multiple pages)*

	Proposed model	**The Mapping Model of Cloud Security and Compliance**	**Simple Cloud Security Model by CSA**
Ability to map cloud security threats and cloud regulatory compliance standards	Compliant	Compliant	Not Compliant – Not Covered
Ability to assess cloud threats with cloud regulatory	Compliant	Moderately Complaint – Model doesn't provide a clear way to assess	Moderately Compliant – Model doesn't provide a clear way to assess

compliance standard goals		cloud threats and align them with regulatory compliance standard goals.	cloud threats and align them with regulatory compliance standard goals.
Adaptability	Compliant	Not Compliant – The model is outdated with the recent evolvements in cloud computing and cloud threat landscape.	Not Complaint – Not covered
Practicality and understandability	Complaint	Not Complaint – The model doesn't include a well-structured mechanism for practical implementation.	Not Complaint - The model doesn't include a well-structured mechanism for practical implementation.
Uniqueness	Complaint	Not Complaint – Model covers all cloud service models and too generic.	Not Complaint – Model covers all cloud service models and too generic.
Coverage	Complaint	Moderately Complaint – Model covers some components of SaaS cloud systems. But doesn't include components specifically focusing on management	Not Complaint – Not covered

		layer of cloud service providers.	

5.4 – Limitations identified in the research

Following points can be highlighted as the limitations identified within this research attempt,

- The data set used for the ML model training step in the implementation phase were collected from a targeted audience. The audience included Sri Lankan IT sector employees working or had prior experience working with cloud-based software systems. The data were collected from them with prior assumption that they are aware about the cloud threats and regulatory compliance standards domain.

- The survey used for data collection process consisted a substantially long set of survey questions which made the survey completion a time-consuming task for the respondents. The survey response collection process could have been improved by doing the response collection in several phases other than in just one single attempt.

- The proposed model and the implementation haven't been tested out within the real world to measure and assess its success rate. This can be only achieved after exposing this model and the implementation to real world.

5.5 – Conclusive remarks

The Analysis and Findings chapter was structured into two main parts. The first part included an analysis and observation of the final implementation and how it achieves the end goal of meeting the research objectives along with a summary and analysis of the survey data collection results. The results obtained by testing the final implementation based on test scenarios created by taking different user personas into account showcased how the final implementation enables a novel way of interacting with the proposed reference model. The survey results findings section showcased the validity of the data collected from survey respondents as the data obtained from the survey plays a significant role in the implementation.

The second part included the benchmarking between the proposed reference model and the reviewed models followed by the limitations of the research.

6 – CONCLUSION

The main output of this research project was creating enhanced cloud security and the compliance reference model for emerging SaaS-based businesses that are consuming public cloud services. Other than the main output, several other vital components were also developed and implemented within this research project to make the primary outcome a unique one compared to already existing solutions deployed commercially or covered in previous research attempts.

The first vital component was the development of the STRIDE-LM+, a unique threat modelling approach proposed to identify and categorize different cloud threats unique to SaaS businesses. This plays a vital role in allowing technical teams within SaaS businesses to assess, plan, and mitigate cloud threats and ensure they are secure and compliant against cloud threats. The Methodology chapter mainly covered the development of the STRIDE-LM+ threat model as it's a significant step integrated within the proposed reference model. The 5-step subprocess that each step within Step 3 of the proposed reference model go through were based on the proposed STRIDE-LM+ threat modelling approach.

The second vital component was the final implementation which includes the API service and machine learning models developed per the final categories identified within the implementation phase. This can be considered a first-of-its-kind approach that exposes a full-fledged API service that provides insights and recommendations on cloud security and compliance status for users based on a reference model. This makes the proposed reference model a far more practical and effective solution for the technical teams within emerging SaaS platforms to continuously assess, improve and maintain their cloud security and compliance status. Machine learning techniques were used to develop the core recommendation and insight generation engine to make this solution adaptable, scalable, and future-proof. The development of machine learning models were based on real-world data collected as a part of this research project.

The vital components discussed above and the main output of this research project enabled meeting the research objectives and provided a clear answer to the research question. Compared to existing research reviewed under the Literature Review chapter, the proposed

reference model and the final implementation can be identified as novel innovations in the cloud security and compliance domain. Even though this research focus has been on creating a solution mainly targeted toward emerging businesses in the SaaS domain, the proposed reference model can also be consumed by enterprise SaaS businesses to assess, improve, and maintain their cloud security and compliance status. The implementation allows any team in their SaaS business journey to easily interact with the proposed reference model and adhere to it despite their experience in cloud security controls and regulatory compliance standards. The Analysis and Findings chapter also proves the final implementation's effectiveness and high accuracy.

When looking into the limitations of the implementation, though steps were taken to ensure that the cluster interpretations always give a better sense to the end-user, there may be scenarios where cluster prediction would misbehave. As the data used to develop the machine learning model included real-world data, this is often expected. This could be only rectified by obtaining a richer data set from a wider global audience. But due to the time and resource limitations of this research project, I had to proceed with the minimum available data set for the implementation. Also, the length of the survey questions could be a reason for this though substantial effort has been taken to reduce the number of audit questions. Since the audit questions cover every dimension within the cloud environment and are based on existing studies, reducing the number of audit questions further was challenging.

6.1 – Future Work

Considering the above limitations, exposing the API service as a product for the end-user and opening it to the world will increase the chance of collecting a richer and more accurate data set, which will improve the cluster prediction capability of the machine learning models. This can be considered an immediate improvement that can be looked upon in future work. Extending the API capability to include the mapping to other existing regulatory and compliance standards can also be identified as an essential step that could further improve the effectiveness of the implementation. On the machine learning side, the clustering technique used within the machine learning model can be enhanced to more accurate algorithms falling under the neural network method for cluster analysis. SOM is considered one of the most popular neural network methods for cluster analysis [57]. It has also been proven that neural

network methods have low error rates [58] and are expected to perform better for cluster analysis than the KModes clustering technique. As we interact with data expected to grow dynamically, a neural network-based clustering technique like GSOM would be ideal for this process. Since it includes the capability to visualize data into a 2D map, it would provide the ability to retrieve better insights into the data and improve the cluster interpretation part [59].

The source code of the API implementation and the training dataset is released to the public under an MIT license and can be viewed under Appendix M.

REFERENCES

[1] Gartner, “Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019,” *gartner.com*, 2019. https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g (accessed Jan. 13, 2020).

[2] CSA, “Cloud Controls Matrix (CCM) - Cloud Controls Matrix 3.0.1,” 2013. https://cloudsecurityalliance.org/group/cloud-controls-matrix/ (accessed Jan. 13, 2020).

[3] “Top Threats to Cloud Computing The Egregious 11,” 2019.

[4] “NIST Cloud Computing Standards Roadmap,” Gaithersburg, MD, Jul. 2013. doi: 10.6028/NIST.SP.500-291r2.

[5] ITU-T, “Y.3502 - Information technology — Cloud computing - Reference architecture.” p. 62, 2014.

[6] A. Rosscow, “The Birth Of GDPR: What Is It And What You Need To Know,” *Forbes*, 2018. https://www.forbes.com/sites/andrewrossow/2018/05/25/the-birth-of-gdpr-what-is-it-and-what-you-need-to-know/#583bee4655e5 (accessed Jan. 13, 2020).

[7] *Bill Text - AB-375 Privacy: personal information: businesses.* 2018.

[8] “Cloud Computing Tops List of Emerging Risks - Smarter With Gartner.” https://www.gartner.com/smarterwithgartner/cloud-computing-tops-list-of-emerging-risks/ (accessed Nov. 30, 2019).

[9] A. Hendre and K. P. Joshi, “A Semantic Approach to Cloud Security and Compliance,” in *Proceedings - 2015 IEEE 8th International Conference on Cloud Computing, CLOUD 2015*, Aug. 2015, pp. 1081–1084. doi: 10.1109/CLOUD.2015.157.

[10] T. Armerding, “Regulatory compliance challenges overwhelm companies | Synopsys.” https://www.synopsys.com/blogs/software-security/regulatory-compliance-challenges/ (accessed Jan. 12, 2020).

[11] D. Yimam and E. B. Fernandez, “Building Compliance and Security Reference Architectures (CSRA) for cloud systems,” in *Proceedings - 2016 IEEE International Conference on Cloud Engineering, IC2E 2016: Co-located with the 1st IEEE International Conference on Internet-of-Things Design and Implementation, IoTDI 2016*, Jun. 2016, pp. 147–150. doi: 10.1109/IC2E.2016.16.

[12] D. Yimam and E. B. Fernandez, “A survey of compliance issues in cloud computing,” *Journal of Internet Services and Applications*, vol. 7, no. 1, Dec. 2016, doi: 10.1186/s13174-016-0046-8.

[13] Michaela Iorga, “The Foundation for Interoperable and Portable Security Automation is Revealed in NIST’s OSCAL Project | NIST,” 2021. https://www.nist.gov/blogs/cybersecurity-insights/foundation-interoperable-and-portable-security-automation-revealed (accessed Jan. 29, 2022).

[14] M. Howard, “Threat Modeling,” in *Security for Software Engineers*, 2019, pp. 170–190. doi: 10.1201/9780429506475-12.

[15] V. E. Urias, B. Van Leeuwen, W. M. S. Stout, and H. Lin, “Applying a Threat Model to Cloud Computing,” in *Proceedings - International Carnahan Conference on Security Technology*, 2018, vol. 2018-Octob. doi: 10.1109/CCST.2018.8585471.

[16] M. Kazim and D. Evans, “Threat modeling for services in cloud,” in *Proceedings - 2016 IEEE Symposium on Service-Oriented System Engineering, SOSE 2016*, May 2016, pp. 84–90. doi: 10.1109/SOSE.2016.55.

[17] S. Manzoor, H. Zhang, and N. Suri, “Threat modeling and analysis for the cloud ecosystem,” in *Proceedings - 2018 IEEE International Conference on Cloud Engineering, IC2E 2018*, May 2018, pp. 278–281. doi: 10.1109/IC2E.2018.00056.

[18] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” *Journal of Network and Computer Applications*, vol. 34, no. 1. pp. 1–11, Jan. 2011. doi: 10.1016/j.jnca.2010.07.006.

[19] D. R. Bharadwaj, A. Bhattacharya, and M. Chakkaravarthy, “Cloud Threat Defense - A Threat Protection and Security Compliance Solution,” in *Proceedings - 7th IEEE International Conference on Cloud Computing in Emerging Markets, CCEM 2018*, Feb. 2019, pp. 95–99. doi: 10.1109/CCEM.2018.00024.

[20] C. M. R. Da Silva, J. L. C. Da Silva, R. B. Rodrigues, G. M. M. Campos, L. M. Do Nascimento, and V. C. Garcia, “Security threats in cloud computing models: Domains and proposals,” in *IEEE International Conference on Cloud Computing, CLOUD*, 2013, pp. 383–389. doi: 10.1109/CLOUD.2013.125.

[21] “CLOUD SECURITY ALLIANCE The Treacherous 12-Top Threats to Cloud Computing + Industry Insights,” 2017.

[22] R. Mogull, J. Arlen, F. Gilbert, A. Lane, D. Mortman, G. Perterson, and M. Rothman, "Security Guidance for Critical Areas of Focus in Cloud Computing v.4.0," pp. 1–152, 2017.

[23] "Introduction to regulatory compliance - Cloud Adoption Framework | Microsoft Docs." https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/policy-compliance/regulatory-compliance (accessed Feb. 25, 2020).

[24] W. Stallings, "Handling of Personal Information and Deidentified, Aggregated, and Pseudonymized Information under the California Consumer Privacy Act," *IEEE Security and Privacy*, vol. 18, no. 1, pp. 61–64, Jan. 2020, doi: 10.1109/MSEC.2019.2953324.

[25] McAfee, "Beyond the General Data Protection Regulation (GDPR): Data residency insights from around the world," 2017.

[26] Consumers International, "The state of data protection rules around the world," 2019.

[27] NIST, "Guidelines on Security and Privacy in Public Cloud Computing," 2011. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf (accessed Mar. 02, 2020).

[28] "Understanding DISA STIG Compliance Requirements | SolarWinds." https://www.solarwinds.com/federal-government/solution/disa-stig-compliance (accessed Mar. 09, 2020).

[29] "FedRAMP Compliance: What is it? Requirements, Process & More!" https://linfordco.com/blog/fedramp-compliance/ (accessed Mar. 09, 2020).

[30] "DMTF Releases Cloud Auditing Data Federation Standard | DMTF." https://www.dmtf.org/news/pr/2014/6/dmtf-releases-cloud-auditing-data-federation-standard (accessed Mar. 09, 2020).

[31] Andrew Miller, "ISO 17799 and 27001: Setting the Standards for Information Security," 2006. https://www.bankinfosecurity.com/iso-17799-27001-setting-standards-for-information-security-a-165 (accessed Mar. 09, 2020).

[32] F. 140-2, "FIPS 140-2 Security requirements for cryptographic modules," 2016.

[33] PCISSC, "Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards," *PCI Security Standards Council*, 2018. https://www.pcisecuritystandards.org/ (accessed Mar. 09, 2020).

[34] “Summary of the HIPAA Security Rule | HHS.gov,” *hhs.gov*, 2017. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (accessed Mar. 09, 2020).

[35] “Knock your SOX off: Federal compliance rules and the cloud.” http://techgenix.com/sox-compliance-cloud/ (accessed Mar. 09, 2020).

[36] “MPAA Compliance - Amazon Web Services (AWS).” https://aws.amazon.com/compliance/mpaa/ (accessed Mar. 09, 2020).

[37] “What is SOC 2 | Guide to SOC 2 Compliance & Certification | Incapsula.” https://www.imperva.com/learn/data-security/soc-2-compliance/ (accessed Mar. 09, 2020).

[38] M. Rouse, “What is EDRM (electronic discovery reference model)? - Definition from WhatIs.com.” https://searchcompliance.techtarget.com/definition/EDRM-electronic-discovery-reference-model (accessed Mar. 09, 2020).

[39] B. Russo, L. Valle, G. Bonzagni, D. Locatello, M. Pancaldi, and D. Tosi, “Cloud Computing and the New EU General Data Protection Regulation,” *IEEE Cloud Computing*, vol. 5, no. 6, pp. 58–68, Nov. 2018, doi: 10.1109/MCC.2018.064181121.

[40] M. Korolov, “California Consumer Privacy Act (CCPA): What you need to know to be compliant,” *CSO (Online)*, 2019.

[41] “Why Use NIST 800-53? | Apptega.” https://www.apptega.com/blog/why-consider-nist-800-53-certification (accessed Feb. 14, 2022).

[42] E. Rios, E Iturbe, X Larrucea, M Rak, W Mallouli, J Dominiak, V Muntés, P Matthews, and L Gonzalez, “Service level agreement-based GDPR compliance and security assurance in (multi)Cloud-based systems,” *IET Software*, vol. 13, no. 3, pp. 213–222, Jun. 2019, doi: 10.1049/iet-sen.2018.5293.

[43] L. Elluri and K. P. Joshi, “A knowledge representation of cloud data controls for eu gdpr compliance,” in *Proceedings - 2018 IEEE World Congress on Services, SERVICES 2018*, Oct. 2018, pp. 47–48. doi: 10.1109/SERVICES.2018.00036.

[44] F. S. Al-Anzi, S. K. Yadav, and J. Soni, “Cloud computing: Security model comprising governance, risk management and compliance,” in *2014 International Conference on Data Mining and Intelligent Computing (ICDMIC)*, Sep. 2014, pp. 1–6. doi: 10.1109/ICDMIC.2014.6954232.

[45] J. Che, Y. Duan, T. Zhang, and J. Fan, “Study on the security models and strategies of cloud computing,” in *Procedia Engineering*, 2011, vol. 23, pp. 586–593. doi: 10.1016/j.proeng.2011.11.2551.

[46] “Consensus Assessment Initiative Questionnaire (CAIQ) v3.1 | CSA.” https://cloudsecurityalliance.org/artifacts/consensus-assessments-initiative-questionnaire-v3-1/ (accessed Feb. 20, 2022).

[47] “CAIQ-Lite | CSA.” https://cloudsecurityalliance.org/star/caiq-lite/ (accessed Feb. 20, 2022).

[48] F. Cao, J. Liang, and L. Bai, “A new initialization method for categorical data clustering”, doi: 10.1016/j.eswa.2009.01.060.

[49] S. Bhat, C. J.M Brook, B Calguner, T Eliyahu, A Getzin, V Hargrave, E Osime, M Roza, J Yeoh, and N Yousif “Top Threats to Cloud Computing: Egregious Eleven Deep Dive,” 2020. [Online]. Available: https://circle.cloudsecurityalliance.org/community-home1?CommunityKey=202830f1-b186-4b55-8c48-

[50] “Understanding Machine Learning - Machine Learning for Software Engineers.” https://www.educative.io/module/lesson/ml-for-software-engineers/RM6BpGzA9v0 (accessed Mar. 02, 2022).

[51] “Consensus Assessment Initiative Questionnaire (CAIQ) v3.1 | CSA.” https://cloudsecurityalliance.org/artifacts/consensus-assessments-initiative-questionnaire-v3-1/ (accessed Mar. 15, 2022).

[52] “A Quick Overview - Machine Learning for Software Engineers.” https://www.educative.io/module/lesson/ml-for-software-engineers/g2yJGmEwWJZ (accessed Mar. 02, 2022).

[53] “Introduction - Machine Learning for Software Engineers.” https://www.educative.io/module/lesson/ml-for-software-engineers/xVX1D6PkRO9 (accessed Mar. 02, 2022).

[54] “DevSecOps.” https://www.devsecops.org/ (accessed Mar. 11, 2022).

[55] “SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC.” https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (accessed Jan. 30, 2022).

[56] “Interpret Results and Adjust Clustering | Clustering in Machine Learning | Google Developers.” https://developers.google.com/machine-learning/clustering/interpret (accessed Mar. 20, 2022).

[57] L. Yang, Z. Ouyang, and Y. Shi, “A modified clustering method based on self-organising maps and its applications,” *Procedia Computer Science*, vol. 9, pp. 1371–1379, 2012, doi: 10.1016/J.PROCS.2012.04.151.

[58] H. Atil and A. Akilli, “Comparison of artificial neural network and K-means for clustering dairy cattle,” *International Journal of Sustainable Agricultural Management and Informatics*, vol. 2, no. 1, pp. 40–52, 2016, doi: 10.1504/IJSAMI.2016.077266.

[59] D. Alahakoon, S. K. Halgamuge, and B. Srinivasan, “Dynamic Self-Organizing Maps with Controlled Growth for Knowledge Discovery,” 2000.

APPENDICES

Appendix A - Mapping between the latest CSA top most cloud threats and the CSA Cloud control domains

		Data Breaches	Misconfiguration and Inadequate Change Control	Lack of Cloud Security Architecture and Strategy	Insufficient Identity, Credential, Access and Key Management	Account Hijacking	Insider Threat	Insecure Interface and APIs	Weak Control Plane	Metastructutre and Applistructure Failures (CSP/customer line of demarcation—also known as the waterline.)	Limited Cloud Usage Visibility	Abuse and Nefarious Use of Cloud Services
Control Domain	**CCM V3.0.1 Control ID**											
Application & Interface Security Application Security	AIS-01	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE
Application & Interface Security Customer Access Requirements	AIS-02	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE
Application & Interface Security Data Integrity	AIS-03	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	FALSE	FALSE
Application & Interface Security Data Security / Integrity	AIS-04	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	FALSE	FALSE
Audit Assurance & Compliance Audit Planning	AAC-01	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE
Audit Assurance & Compliance Independent Audits	AAC-02	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Audit Assurance & Compliance Information System Regulatory Mapping	AAC-03	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE

Business Continuity Management & Operational Resilience Business Continuity Planning	BCR-01	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Business Continuity Management & Operational Resilience Business Continuity Testing	BCR-02	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE
Business Continuity Management & Operational Resilience Datacenter Utilities / Environmental Conditions	BCR-03	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Business Continuity Management & Operational Resilience Documentation	BCR-04	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE	FALSE
Business Continuity Management & Operational Resilience Environmental Risks	BCR-05	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Business Continuity Management & Operational Resilience Equipment Location	BCR-06	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Business Continuity Management & Operational Resilience Equipment Maintenance	BCR-07	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Business Continuity	BCR-08	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE

Management & Operational Resilience Equipment Power Failures												
Business Continuity Management & Operational Resilience Impact Analysis	BCR-09	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE
Business Continuity Management & Operational Resilience Policy	BCR-10	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Business Continuity Management & Operational Resilience Retention Policy	BCR-11	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Change Control & Configuration Management New Development / Acquisition	CCC-01	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE
Change Control & Configuration Management Outsourced Development	CCC-02	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE
Change Control & Configuration Management Quality Testing	CCC-03	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Change Control & Configuration Management Unauthorized Software Installations	CCC-04	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Change Control & Configuration Management Production Changes	CCC-05	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE
Data Security & Information Lifecycle Management Classification	DSI-01	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE

Data Security & Information Lifecycle Management Data Inventory / Flows	DSI-02	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE
Data Security & Information Lifecycle Management Ecommerce Transactions	DSI-03	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Data Security & Information Lifecycle Management Handling / Labeling / Security Policy	DSI-04	TRUE	TRUE	FALSE	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE	TRUE
Data Security & Information Lifecycle Management Non-Production Data	DSI-05	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Data Security & Information Lifecycle Management Ownership / Stewardship	DSI-06	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	TRUE	FALSE
Data Security & Information Lifecycle Management Secure Disposal	DSI-07	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Datacenter Security Asset Management	DCS-01	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Datacenter Security Controlled Access Points	DCS-02	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Datacenter Security Equipment Identification	DCS-03	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Datacenter Security Off-Site Authorization	DCS-04	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE

Datacenter Security Off-Site Equipment	DCS-05	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Datacenter Security Policy	DCS-06	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Datacenter Security Secure Area Authorization	DCS-07	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Datacenter Security Unauthorized Persons Entry	DCS-08	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Datacenter Security User Access	DCS-09	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Encryption & Key Management Entitlement	EKM-01	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Encryption & Key Management Key Generation	EKM-02	TRUE	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
Encryption & Key Management Sensitive Data Protection	EKM-03	TRUE	TRUE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	TRUE	TRUE
Encryption & Key Management Storage and Access	EKM-04	TRUE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Governance and Risk Management Baseline Requirements	GRM-01	FALSE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE
Governance and Risk Management Data Focus Risk Assessments	GRM-02	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE
Governance and Risk Management Management Oversight	GRM-03	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	TRUE	FALSE
Governance and Risk Management Management Program	GRM-04	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE

Governance and Risk Management Management Support/Involvement	GRM-05	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Governance and Risk Management Policy	GRM-06	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE
Governance and Risk Management Policy Enforcement	GRM-07	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE
Governance and Risk Management Policy Impact on Risk Assessments	GRM-08	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE
Governance and Risk Management Policy Reviews	GRM-09	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE
Governance and Risk Management Risk Assessments	GRM-10	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE
Governance and Risk Management Risk Management Framework	GRM-11	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE
Human Resources Asset Returns	HRS-01	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Human Resources Background Screening	HRS-02	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
Human Resources Employment Agreements	HRS-03	FALSE	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	TRUE	FALSE
Human Resources Employment Termination	HRS-04	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Human Resources	HRS-05	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE

Mobile Device Management												
Human Resources Non-Disclosure Agreements	HRS-06	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Human Resources Roles / Responsibilities	HRS-07	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	TRUE	FALSE
Human Resources Technology Acceptable Use	HRS-08	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE
Human Resources Training / Awareness	HRS-09	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE
Human Resources User Responsibility	HRS-10	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE
Human Resources Workspace	HRS-11	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Identity & Access Management Audit Tools Access	IAM-01	TRUE	FALSE	FALSE	TRUE	FALSE	TRUE	TRUE	FALSE	TRUE	FALSE	FALSE
Identity & Access Management Credential Lifecycle / Provision Management	IAM-02	FALSE	TRUE	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	TRUE	FALSE	TRUE
Identity & Access Management Diagnostic / Configuration Ports Access	IAM-03	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Identity & Access Management Policies and Procedures	IAM-04	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE
Identity & Access Management Segregation of Duties	IAM-05	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	TRUE
Identity & Access Management Source Code Access Restriction	IAM-06	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE

Identity & Access Management Third Party Access	IAM-07	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE
Identity & Access Management Trusted Sources	IAM-08	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	FALSE	TRUE	FALSE	FALSE
Identity & Access Management User Access Authorization	IAM-09	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE
Identity & Access Management User Access Reviews	IAM-10	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	TRUE
Identity & Access Management User Access Revocation	IAM-11	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	FALSE	TRUE	FALSE	TRUE
Identity & Access Management User ID Credentials	IAM-12	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE
Identity & Access Management Utility Programs Access	IAM-13	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE
Infrastructure & Virtualization Security Audit Logging / Intrusion Detection	IVS-01	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	TRUE	TRUE	FALSE	FALSE	TRUE
Infrastructure & Virtualization Security Change Detection	IVS-02	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE
Infrastructure & Virtualization Security Clock Synchronization	IVS-03	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Infrastructure & Virtualization Security Information System Documentation	IVS-04	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE
Infrastructure & Virtualization Security	IVS-05	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE

Vulnerability Management												
Infrastructure & Virtualization Security Network Security	IVS-06	FALSE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE
Infrastructure & Virtualization Security OS Hardening and Base Controls	IVS-07	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Infrastructure & Virtualization Security Production / Non-Production Environments	IVS-08	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Infrastructure & Virtualization Security Segmentation	IVS-09	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	TRUE	TRUE	FALSE	FALSE
Infrastructure & Virtualization Security VM Security - Data Protection	IVS-10	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Infrastructure & Virtualization Security Hypervisor Hardening	IVS-11	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Infrastructure & Virtualization Security Wireless Security	IVS-12	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Infrastructure & Virtualization Security Network Architecture	IVS-13	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE
Interoperability & Portability APIs	IPY-01	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE
Interoperability & Portability Data Request	IPY-02	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Interoperability & Portability Policy & Legal	IPY-03	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Interoperability & Portability Standardized	IPY-04	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE

Network Protocols												
Interoperability & Portability Virtualization	IPY-05	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Mobile Security Anti-Malware	MOS-01	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Mobile Security Application Stores	MOS-02	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Mobile Security Approved Applications	MOS-03	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Mobile Security Approved Software for BYOD	MOS-04	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Mobile Security Awareness and Training	MOS-05	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Mobile Security Cloud Based Services	MOS-06	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Mobile Security Compatibility	MOS-07	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Mobile Security Device Eligibility	MOS-08	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Mobile Security Device Inventory	MOS-09	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Mobile Security Device Management	MOS-10	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Mobile Security Encryption	MOS-11	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Mobile Security Jailbreaking and Rooting	MOS-12	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Mobile Security Legal	MOS-13	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Mobile Security Lockout Screen	MOS-14	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Mobile Security Operating Systems	MOS-15	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Mobile Security Passwords	MOS-16	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Mobile Security Policy	MOS-17	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Mobile Security Remote Wipe	MOS-18	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE

Mobile Security Security Patches	MOS-19	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Mobile Security Users	MOS-20	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Security Incident Management, E-Discovery, & Cloud Forensics Contact / Authority Maintenance	SEF-01	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Security Incident Management, E-Discovery, & Cloud Forensics Incident Management	SEF-02	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Security Incident Management, E-Discovery, & Cloud Forensics Incident Reporting	SEF-03	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Security Incident Management, E-Discovery, & Cloud Forensics Incident Response Legal Preparation	SEF-04	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE
Security Incident Management, E-Discovery, & Cloud Forensics Incident Response Metrics	SEF-05	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Supply Chain Management, Transparency, and Accountability Data Quality and Integrity	STA-01	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Supply Chain Management, Transparency, and Accountability Incident Reporting	STA-02	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Supply Chain Management, Transparency,	STA-03	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE

and Accountability Network / Infrastructure Services												
Supply Chain Management, Transparency, and Accountability Provider Internal Assessments	STA-04	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Supply Chain Management, Transparency, and Accountability Supply Chain Agreements	STA-05	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Supply Chain Management, Transparency, and Accountability Supply Chain Governance Reviews	STA-06	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Supply Chain Management, Transparency, and Accountability Supply Chain Metrics	STA-07	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Supply Chain Management, Transparency, and Accountability Third Party Assessment	STA-08	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Supply Chain Management, Transparency, and Accountability Third Party Audits	STA-09	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
Threat and Vulnerability Management Anti-Virus / Malicious Software	TVM-01	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE

Threat and Vulnerability Management Vulnerability / Patch Management	TVM-02	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE
Threat and Vulnerability Management Mobile Code	TVM-03	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE

Appendix B – Generic Survey Question Set

- Select the type of the business
- Number of Employees
- Your job area
- Your job level
- What is the business domain of the SaaS business?
- What are the geographical locations of your targeted customer base? (Select All that apply)
- Are you aware of regulatory compliance standards applicable to your SaaS business? (If yes, select all that applies)
- What is the cloud deployment method/ model used by the SaaS platform?
- What are the cloud service providers consumed by the SaaS platform? (If multiple cloud service providers are used, select all that apply)
- Do you evaluate and review the shared responsibility model of your cloud service provider and clearly understands which party is accountable (you and your cloud service provider) for security and compliance obligations?

Appendix C - Mapping between the survey questions under Assessing SaaS Cloud system resources to each subcategory within Step 3 of the proposed reference model

	Assessing Identity and Access Management (3.A)	**Type [Governance (G)/ Operations (O)]**
	IAM	
A1	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.) including ones which are hosted within public cloud services you consume (e.g., AWS Security Hub, GCP The Cloud Security Command Center, AWS Security Center etc.)?	O
A2	Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	O
A3	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	G
A4	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	G
A5	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?	O
A6	Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?	O
A7	Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege?	G
A8	Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (exclusive of users maintained by your tenants), based on the rule of least privilege, by business leadership or other accountable business role or function?	O
A9	Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?	O
	Assessing Metastructure (3.B)	
	EKM	

B1	Do you have a capability to allow creation of unique encryption keys per tenant?	O
B2	Do you encrypt tenant data at rest (on disk/storage) within your environment?	O
	HRS	
B3	Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-owned assets?	G
B4	In accordance to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?	G
B5	Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies?	G
B6	Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?	G
B7	Are personnel trained and provided with awareness programs at least once a year?	G
	AAC	
B8	Do you allow tenants to view your third-party audit or certification reports?	G
B9	Do you conduct network penetration tests of your cloud service infrastructure at least annually?	O
B10	Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	O
B11	Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	G
	CCC	
B12	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	O
	SEF	
B13	Are you aware of necessary points of contacts with your CSP for IR escalation and support?	G

B14	Do you have a documented security incident response plan and test it regularly (at least annually)?	G
B15	Are workforce personnel and external business relationships adequately informed of their responsibility, and, if required, consent and/or contractually required to report all information security events in a timely manner?	G
B16	Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations?	O
	BCR	
B17	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	G
B18	Do you have technical capabilities to enforce tenant data retention policies?	O
B19	Have you identified your critical assets required for the functioning of your system and implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	O
B20	Do you test your backup or redundancy mechanisms at least annually?	O
	GRM	
B21	Do you have identified and enabled the information security baselines for every component of your cloud infrastructure and services?	G
B22	Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/function and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)?	G
B23	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	G
B24	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	G
B25	Do you perform, at minimum, annual reviews to your privacy and security policies?	G
	Assessing Applistructure and Infostructure (3.C)	

	AIS	
C1	Do you use an automated source code analysis tool to detect security defects in code prior to production?	O
C2	Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	O
C3	Are all information related to security, contractual and regulatory requirements for customer access are clearly shared, addressed, remediated prior to granting customers access to your SaaS platform?	G
C4	Does your data management policies and procedures require audits to verify data input and output integrity routines?	G
	IPY	
C5	Do you publish a list of all APIs available in the service and has proper documentation indicating which are standard and which are customized?	G
	DSI	
C6	Do you provide standardized (e.g. ISO/IEC) non-proprietary encryption algorithms (3DES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	O
C7	Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	O
C8	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	G
C9	Do you support the secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data (You can answer yes if your public CSP is responsible for this control and adheres by it)?	G
C10	Do you have a published procedure in data deletion controls in place after a tenant/ customer exits the service agreement?	G
	Assessing Infrastructure (3.D)	
	IVS	
D1	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?	O
D2	Is logical user access to audit logs restricted to authorized personnel?	G

D3	Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	O
D4	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?	O
D5	For your SaaS offering, do you provide tenants with separate environments for production and test processes?	O
D6	Do you logically segregate production and non-production environments?	O
D7	Do you restrict personnel access to all administrative consoles for systems hosting cloud virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	G
	TVM	
D8	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your IT infrastructure network and systems components?	O
D9	Do you have a capability to patch vulnerabilities across all of your computing devices, applications, and systems?	O

Appendix D – Category A | Governance Dataset Cluster Breakdown

	A3	A4	A7	Clusters
0	1	1	1	0
1	1	1	1	0
2	0	1	1	0
3	0	0	0	1
4	1	1	1	0
5	1	1	1	0
6	0	1	1	0
7	1	1	1	0
8	0	0	1	2
9	0	1	0	1
10	1	1	0	0
11	0	0	1	2
12	0	0	0	1
13	1	1	1	0
14	1	1	1	0
15	1	0	0	0
16	0	0	1	2
17	1	1	1	0
18	0	1	2	1
19	1	1	0	0
20	1	1	1	0

	A3	A4	A7	Clusters
21	1	1	1	0
22	1	1	1	0
23	1	1	1	0
24	0	1	0	1
25	1	0	1	0
26	1	1	1	0
27	1	1	1	0
28	1	1	1	0
29	1	1	0	0
30	1	1	1	0
31	1	1	1	0
32	0	1	1	0
33	1	0	1	0
34	1	1	1	0
35	1	1	1	0
36	0	1	1	0
37	1	0	0	0
38	0	1	2	1
39	1	0	1	0
40	1	1	1	0
41	1	1	1	0
42	1	1	0	0

	A3	A4	A7	Clusters
43	0	0	0	1
44	1	1	1	0
45	1	1	0	0
46	1	1	1	0
47	1	1	1	0
48	1	1	1	0
49	1	1	1	0
50	1	1	1	0

Appendix E - Category A | Operations Dataset Cluster Breakdown

	A1	A2	A5	A6	A8	A9	Clusters
0	1	1	1	1	1	1	0
1	1	1	1	1	1	1	0
2	1	1	1	1	0	0	2
3	0	0	0	0	0	0	1
4	1	1	1	1	1	1	0
5	0	0	1	1	1	1	0
6	1	1	1	1	0	1	0
7	1	1	1	0	1	1	0
8	1	1	1	1	0	0	2
9	0	1	1	1	0	1	0
10	1	1	1	1	0	1	0
11	1	1	1	1	0	0	2
12	0	0	0	0	0	0	1
13	1	1	1	1	1	1	0
14	1	1	1	1	1	1	0
15	1	1	0	1	1	1	0
16	0	0	0	1	0	0	1
17	1	1	1	1	1	1	0
18	1	1	1	2	0	0	2

	A1	A2	A5	A6	A8	A9	Clusters
19	1	1	1	1	0	1	0
20	1	1	1	1	1	1	0
21	1	1	1	1	1	1	0
22	0	0	1	1	1	1	0
23	1	0	1	1	0	1	3
24	1	1	1	1	0	0	2
25	1	0	1	1	1	1	0
26	1	1	1	1	1	1	0
27	1	1	1	1	1	1	0
28	0	1	1	1	1	1	0
29	1	1	1	1	0	1	0
30	1	1	1	1	1	1	0
31	1	1	1	1	1	1	0
32	1	1	1	1	0	0	2
33	1	1	1	1	1	1	0
34	1	1	1	1	1	1	0
35	1	1	1	1	1	1	0
36	0	0	0	0	0	0	1
37	1	1	0	0	1	1	0

	A1	A2	A5	A6	A8	A9	Clusters
38	0	0	0	0	0	0	1
39	1	1	0	0	1	1	0
40	1	0	1	1	1	1	0
41	1	0	1	1	0	1	3
42	1	1	1	1	1	1	0
43	0	0	0	0	0	0	1
44	1	0	1	1	0	1	3
45	1	1	1	1	0	1	0
46	1	1	1	1	0	1	0
47	1	1	1	1	1	1	0
48	1	1	1	1	1	1	0
49	1	1	1	1	1	1	0
50	1	1	1	1	1	1	0

Appendix F - Category B | Governance Dataset Cluster Breakdown

	B3	B4	B5	B6	B7	B8	B11	B13	B14	B15	B17	B21	B22	B23	B24	B25	Clusters
0	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	0
1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	0
2	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	0
3	0	1	1	0	1	2	0	0	0	0	0	0	0	0	0	0	1
4	0	0	0	1	1	0	0	1	0	0	0	0	1	0	1	0	1
5	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	0
6	1	0	1	1	1	0	1	0	0	0	0	0	1	0	1	1	1
7	1	1	0	0	1	2	1	0	1	0	1	1	0	0	0	0	2
8	1	0	1	1	0	0	1	0	0	0	0	0	0	1	1	1	1
9	0	1	0	1	0	1	0	1	0	1	1	1	1	1	1	1	0
10	1	1	1	0	0	0	0	1	0	0	0	0	0	0	1	0	1
11	1	1	1	1	1	1	0	1	0	0	0	0	1	1	1	1	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
13	1	0	1	1	1	0	0	1	1	1	1	1	1	1	1	1	0
14	0	0	1	1	1	0	1	1	1	1	1	1	1	1	1	0	0
15	1	1	1	1	0	0	0	1	0	1	1	0	0	0	1	0	1

	B3	B4	B5	B6	B7	B8	B11	B13	B14	B15	B17	B21	B22	B23	B24	B25	Clusters
16	1	1	1	1	0	2	0	0	1	1	0	0	1	0	1	1	0
17	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0
18	0	0	0	0	0	2	0	0	0	0	0	1	1	0	0	0	2
19	1	1	1	1	0	1	1	1	1	0	0	0	1	0	0	1	0
20	1	1	1	1	1	2	1	1	1	1	1	1	1	1	0	1	0
21	1	0	0	1	1	1	1	1	1	1	1	1	1	1	1	0	0
22	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0
23	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	0
24	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	0
25	0	0	0	0	0	2	0	0	0	0	0	0	1	0	0	0	2
26	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0
27	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0
28	1	0	1	1	1	0	1	1	1	1	1	1	1	1	1	0	0
29	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0
30	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	0
31	1	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	0
32	1	1	1	1	1	1	0	1	1	1	1	0	1	1	1	1	0

	B3	B4	B5	B6	B7	B8	B11	B13	B14	B15	B17	B21	B22	B23	B24	B25	Clusters
33	1	1	1	1	1	1	1	1	1	1	0	1	0	1	1	1	0
34	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0
35	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0
36	0	1	0	0	0	0	0	0	1	0	0	0	0	1	1	1	1
37	0	1	0	0	0	2	0	1	1	0	1	1	0	0	0	0	2
38	0	0	0	0	0	1	0	1	1	0	1	1	0	0	0	1	2
39	0	0	0	0	0	1	1	0	0	0	0	1	1	0	0	1	2
40	1	0	1	1	1	0	0	1	1	1	1	1	0	1	1	1	0
41	1	0	1	1	1	1	0	1	1	1	0	0	0	1	1	0	0
42	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0
43	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	1
44	1	1	1	1	1	1	1	0	0	1	0	1	0	1	1	1	0
45	0	0	0	0	0	0	0	0	1	0	1	0	0	1	1	0	1
46	0	0	0	0	0	0	0	1	1	0	0	1	0	0	0	0	2
47	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	0
48	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0
49	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	0

	B3	B4	B5	B6	B7	B8	B11	B13	B14	B15	B17	B21	B22	B23	B24	B25	Clusters
50	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	0

Appendix G - Category B | Operations Dataset Cluster Breakdown

	B1	B2	B9	B10	B12	B16	B18	B19	B20	Clusters
0	0	0	1	1	1	0	1	1	1	0
1	0	1	1	1	1	1	1	1	1	0
2	1	1	1	1	1	1	1	1	0	0
3	2	2	0	0	0	0	0	0	0	1
4	1	0	1	0	1	0	1	1	1	2
5	2	1	1	1	1	1	1	1	1	0
6	1	0	0	0	0	1	1	1	1	2
7	2	2	1	1	0	0	1	1	1	0
8	0	2	1	0	1	0	0	1	1	0
9	0	0	0	0	0	1	1	1	1	2
10	1	0	0	0	0	0	1	1	0	1
11	0	1	1	0	0	1	1	1	1	0
12	0	0	0	0	0	0	2	0	0	1
13	1	1	0	0	1	1	1	1	1	2
14	2	1	1	1	1	1	1	1	1	0

	B1	B2	B9	B10	B12	B16	B18	B19	B20	Clusters
15	0	0	1	0	1	1	1	0	0	0
16	2	2	0	0	1	1	2	0	0	1
17	1	1	1	1	1	1	1	1	1	0
18	2	2	0	0	0	0	2	0	0	1
19	0	1	0	1	1	1	1	1	0	0
20	1	1	1	1	1	1	1	1	1	0
21	1	1	1	1	1	1	1	1	1	0
22	1	0	1	1	1	1	1	1	1	0
23	0	1	1	1	1	1	1	1	1	0
24	0	1	1	1	0	1	1	1	1	0
25	0	0	0	0	0	0	0	0	0	1
26	0	1	1	1	1	1	1	1	1	0
27	0	0	1	1	1	1	1	1	1	0
28	0	1	0	0	0	1	0	0	0	1
29	0	0	1	1	1	0	1	1	1	0

	B1	B2	B9	B10	B12	B16	B18	B19	B20	Clusters
30	0	1	1	1	1	1	0	0	0	0
31	0	1	0	0	0	1	1	1	1	0
32	0	1	1	1	1	1	1	1	1	0
33	1	1	1	1	1	1	1	1	1	0
34	1	1	1	1	1	1	1	1	1	0
35	1	1	1	1	1	1	1	1	1	0
36	1	2	0	0	1	1	1	1	1	2
37	0	1	0	0	1	0	0	0	0	1
38	1	1	1	1	0	0	2	0	0	1
39	1	1	1	1	0	0	1	1	1	0
40	0	0	0	0	1	1	1	1	1	2
41	0	1	1	1	1	1	0	0	0	0
42	1	1	1	1	1	1	1	1	1	0
43	0	0	0	0	0	0	1	1	1	1
44	0	1	1	1	1	1	1	1	1	0

	B1	B2	B9	B10	B12	B16	B18	B19	B20	Clusters
45	0	0	0	0	1	0	0	0	0	1
46	1	1	0	0	1	0	1	1	1	2
47	1	1	1	1	1	1	1	1	1	0
48	1	1	1	1	1	1	1	1	1	0
49	1	0	1	1	1	1	1	1	1	0
50	1	1	1	1	1	1	1	1	1	0

Appendix H - Category C | Governance Dataset Cluster Breakdown

	C3	C4	C5	C8	C9	C10	Clusters
0	1	1	1	1	1	1	0
1	1	1	1	1	1	1	0
2	1	1	0	1	1	1	0
3	0	0	2	1	1	0	2
4	0	1	0	0	0	0	1
5	1	1	1	1	1	1	0
6	0	0	1	1	1	1	0
7	1	1	1	1	1	1	0
8	1	0	0	0	0	1	1
9	1	0	1	1	1	0	0
10	0	1	1	0	0	0	1
11	1	1	1	1	1	1	0
12	0	0	2	0	1	0	2
13	1	1	1	1	1	1	0
14	1	1	1	1	1	1	0

	C3	C4	C5	C8	C9	C10	Clusters
15	1	0	0	0	1	0	2
16	1	0	2	0	1	0	2
17	1	1	1	1	1	1	0
18	0	0	1	0	1	0	2
19	1	0	0	0	0	1	1
20	0	0	0	1	1	1	1
21	1	1	2	1	1	1	0
22	1	1	1	1	1	1	0
23	0	1	0	1	0	1	1
24	0	1	1	1	1	0	0
25	0	0	0	0	0	0	1
26	1	1	1	1	1	1	0
27	1	1	0	0	0	1	1
28	0	0	0	1	0	1	1
29	0	0	0	1	0	0	1

	C3	C4	C5	C8	C9	C10	Clusters
30	1	1	1	1	1	1	0
31	1	0	1	1	1	1	0
32	1	1	1	1	1	0	0
33	1	1	0	1	1	1	0
34	1	1	1	1	1	1	0
35	1	1	1	1	1	1	0
36	1	0	0	0	0	0	1
37	1	1	1	1	1	1	0
38	0	0	0	0	1	1	1
39	1	1	1	1	1	1	0
40	1	1	0	1	0	0	0
41	0	0	0	0	1	1	1
42	1	1	1	1	1	1	0
43	0	0	0	0	0	0	1
44	0	1	0	1	0	1	1

	C3	C4	C5	C8	C9	C10	Clusters
45	0	0	0	1	0	0	1
46	0	0	0	1	1	1	1
47	1	1	1	1	1	1	0
48	1	1	1	1	1	1	0
49	1	1	1	1	1	1	0
50	1	1	1	1	1	1	0

Appendix I - Category C | Operations Dataset Cluster Breakdown

	C1	C2	C6	C7	Clusters
0	0	1	1	1	0
1	0	1	1	1	0
2	1	1	0	1	0
3	0	0	0	0	1
4	1	1	0	0	3
5	1	1	1	1	0
6	1	1	1	1	0
7	1	1	1	1	0
8	1	1	1	1	0
9	0	1	1	1	0
10	0	1	0	1	2
11	0	1	1	1	0
12	0	0	0	0	1
13	0	1	1	1	0
14	1	1	1	1	0
15	1	1	1	0	0
16	0	1	0	0	1
17	1	1	1	1	0

	C1	C2	C6	C7	Clusters
18	0	1	0	0	1
19	0	0	0	1	1
20	1	0	0	0	1
21	1	1	0	1	0
22	1	1	0	0	3
23	1	1	1	1	0
24	0	0	1	1	4
25	0	0	0	0	1
26	1	1	1	1	0
27	1	1	0	0	3
28	1	1	1	1	0
29	0	0	0	0	1
30	0	0	1	1	4
31	0	0	1	1	4
32	1	1	1	1	0
33	1	1	1	1	0
34	1	1	1	1	0
35	1	1	1	1	0
36	1	1	0	0	3
37	0	0	0	0	1

	C1	C2	C6	C7	Clusters
38	1	1	0	0	3
39	1	1	1	1	0
40	0	0	0	0	1
41	0	0	1	1	4
42	1	1	1	1	0
43	0	0	0	0	1
44	1	1	1	1	0
45	0	0	0	0	1
46	0	0	1	1	4
47	1	1	0	0	3
48	1	1	1	1	0
49	1	1	0	0	3
50	1	1	1	1	0

Appendix J - Category D | Governance Dataset Cluster Breakdown

	D2	D7	Clusters
0	1	1	2
1	1	1	2
2	1	1	2
3	0	0	3
4	1	0	0
5	1	1	2
6	1	1	2
7	1	1	2
8	1	1	2
9	1	1	2
10	1	1	2
11	1	1	2
12	0	0	3
13	1	1	2

	D2	D7	Clusters
14	1	1	2
15	0	1	1
16	1	1	2
17	1	1	2
18	0	0	3
19	1	1	2
20	1	1	2
21	1	1	2
22	1	0	0
23	1	0	0
24	1	1	2
25	0	0	3
26	1	1	2
27	1	1	2
28	0	1	1

	D2	D7	Clusters
29	1	1	2
30	1	1	2
31	1	1	2
32	1	1	2
33	0	1	1
34	1	1	2
35	1	1	2
36	0	0	3
37	0	1	1
38	0	0	3
39	1	1	2
40	0	0	3
41	0	0	3
42	1	1	2
43	0	0	3

	D2	D7	Clusters
44	1	0	0
45	0	1	1
46	0	1	1
47	1	1	2
48	1	1	2
49	1	0	0
50	1	1	2

Appendix K - Category D | Operations Dataset Cluster Breakdown

	D1	D3	D4	D5	D6	D8	D9	Clusters
0	1	1	1	1	1	1	1	0
1	1	1	1	1	1	1	1	0
2	1	0	1	1	1	1	1	0
3	0	0	0	2	1	1	0	3
4	0	1	1	1	0	0	0	1
5	1	1	1	1	1	1	1	0
6	0	1	0	1	1	1	1	0
7	1	1	1	1	1	1	1	0
8	1	1	1	1	1	1	1	0
9	0	0	1	1	1	1	1	0
10	0	0	0	1	1	0	0	1
11	1	1	1	1	1	1	1	0
12	0	0	0	2	0	0	0	1
13	1	1	1	1	1	1	0	0

	D1	D3	D4	D5	D6	D8	D9	Clusters
14	1	1	1	0	1	0	1	0
15	0	0	1	1	1	0	1	0
16	0	0	0	1	1	1	1	3
17	1	1	1	1	1	1	1	0
18	0	0	0	2	0	0	0	1
19	1	0	0	1	1	1	1	0
20	0	1	0	1	1	1	1	0
21	1	1	1	1	1	1	1	0
22	0	1	1	1	1	1	1	0
23	1	0	0	1	1	1	0	3
24	1	0	1	0	1	1	1	0
25	0	0	0	2	0	0	0	1
26	1	1	1	1	1	1	1	0
27	1	1	1	1	1	1	1	0
28	1	1	1	0	1	1	1	0

	D1	D3	D4	D5	D6	D8	D9	Clusters
29	0	0	0	1	1	0	0	1
30	0	1	0	1	1	1	1	0
31	1	1	0	0	1	1	1	0
32	1	0	1	0	1	1	1	0
33	1	1	0	1	1	1	1	0
34	1	1	1	1	1	1	1	0
35	1	1	1	1	1	1	1	0
36	0	0	0	0	0	0	0	1
37	0	0	0	0	0	0	0	1
38	1	0	0	2	0	1	1	2
39	1	1	1	1	1	1	1	0
40	0	0	1	1	1	1	1	0
41	0	0	0	0	1	0	1	1
42	1	1	1	1	1	1	1	0
43	0	0	0	0	0	0	0	1

	D1	D3	D4	D5	D6	D8	D9	Clusters
44	1	1	1	1	1	0	1	0
45	0	1	0	0	0	0	0	1
46	0	0	1	0	1	1	0	3
47	1	1	1	1	0	1	1	0
48	1	1	1	1	1	1	1	0
49	1	1	1	1	1	0	0	0
50	0	1	1	1	1	1	1	0

Appendix L – Mapping between the proposed model and the NIST 800 53 R5 Standard

Proposed reference model Assessing SaaS Cloud System Resources Controls		**NIST 800 53 R5 Mapping**
Assessing Identity Management (3.A)		
A1	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.) including ones that are hosted within public cloud services you consume (e.g., AWS Security Hub, GCP The Cloud Security Command Center, AWS Security Center etc.)?	AC-2 (4) AC-6 AC-6 (1) AC-6 (5) AU-9 AU-9 (4)
A2	Do you monitor and log privileged access (e.g., administrator-level) to information security management systems?	AC-2 (4) AC-6 AC-6 (1) AC-6 (5) AU-9 AU-9 (4)
A3	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	AC-1 AC-2 AC-2 (1) AC-2 (2) AC-3 AC-4 AC-6 IA-1 IA-2 IA-2 (1) IA-2 (2)

		IA-2 (6) IA-4 IA-5 IA-5 (1) IA-5 (2) IA-12 (4) PS-4 PS-5 SC-2
A4	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	AC-1 AC-2 IA-1 IA-2 IA-5 PS-2
A5	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?	AC-3 AC-5 AC-6 CM-5 CM-11 SA-10
A6	Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?	AC-3 AC-5 AC-6 CM-5 CM-11 SA-10
A7	Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege?	IA-2 IA-5
A8	Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system	AC-2 AC-2 (3)

	users and administrators (exclusive of users maintained by your tenants), based on the rule of least privilege, by business leadership or other accountable business role or function?	AC-2 (4) AC-6 AC-1
A9	Is timely de-provisioning, revocation, or modification of user access to the organization's systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?	AC-2 AC-2 (2) AC-2 (3) PS-4 PS-5 PS-7
Assessing Metastructure (3.B)		
B1	Do you have the capability to allow the creation of unique encryption keys per tenant?	SC-12 SC-13
B2	Do you encrypt tenant data at rest (on disk/storage) within your environment?	SC-8 SC-8 (1) SC-13 SC-28
B3	Upon termination of contract or business relationship, are your employees and business partners adequately informed of their obligations for returning organizationally-owned assets?	PS-4
B4	Per local laws, regulations, ethics and contractual constraints are all employment candidates, contractors, and involved third parties subject to background verification?	PS-3
B5	Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies?	PS-6

B6	Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?	PS-2
B7	Are personnel trained and provided with awareness programs at least once a year?	AT-2
B8	Do you allow tenants to view your third-party audit or certification reports?	CA-2 (1) CA-7 (1)
B9	Do you conduct network penetration tests of your cloud service infrastructure at least annually?	CA-2 (1) CA-7 (1)
B10	Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	CA-2 (1) CA-7 (1)
B11	Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	RA-2 PL-2
B12	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	CM-11 SI-7
B13	Are you aware of the necessary points of contact with your CSP (Cloud Service Provider) for IR (Incident Response) escalation and support?	IR-1 IR-4 IR-5 IR-8
B14	Do you have a documented security incident response plan and test it regularly (at least annually)?	IR-1 IR-4 IR-5 IR-8
B15	Are workforce personnel and external business relationships adequately informed of their responsibility, and, if required, consent and/or contractually required to	IR-2 IR-6 SA-9

	report all information security events in a timely manner?	
B16	Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations?	IR-2 IR-6 SA-9
B17	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	CP-4 CP-4 (1) IR-3 IR-3 (2)
B18	Do you have technical capabilities to enforce tenant data retention policies?	SI-12
B19	Have you identified your critical assets required for the functioning of your system and implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	SI-12
B20	Do you test your backup or redundancy mechanisms at least annually?	SI-12
B21	Do you have identified and enabled the information security baselines for every component of your cloud infrastructure and services?	CM-2 CM-3 CM-6 SA-4 SA-10
B22	Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/function and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)?	AC-1 AU-1 AT-1 CM-1 CP-1 IA-1 IR-1

		MA-1 MP-1 PS-1 PE-1 PL-1 RA-1 CA-1 SI-1 SA-1
B23	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	RA-3
B24	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	AC-1 AT-1 AU-1 CA-1 CM-1 CP-1 IA-1 IR-1 MA-1 MP-1 PE-1 PL-1 RA-1 RA-3 SA-1 SC-1 SI-1
B25	Do you perform, at minimum, annual reviews of your privacy and security policies?	AC-1 AT-1 AU-1

		CA-1 CM-1 CP-1 IA-1 IR-1 MA-1 MP-1 PE-1 PL-1 RA-1 RA-3 SA-1 SC-1 SI-1
Assessing Applistructure and Infrastructure (3.C)		
C1	Do you use an automated source code analysis tool to detect security defects in code prior to production?	RA-5 SA-3 SI-2 SI-10
C2	Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	RA-5 SA-3 SI-2 SI-10
C3	Are all information related to security, contractual and regulatory requirements for customer access is shared, addressed, remediated before granting customers access to your SaaS platform?	No mapping

C4	Do your data management policies and procedures require audits to verify data input and output integrity routines?	SI-10
C5	Do you publish a list of all APIs available in the service and has proper documentation indicating which are standard and which are customized?	No mapping
C6	Do you provide standardized (e.g. ISO/IEC) non-proprietary encryption algorithms (3DES, AES, etc.) to tenants for them to protect their data if it is required to move through public networks (e.g., the Internet)?	RA-2 SC-8 SC-8 (1)
C7	Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	RA-2 SC-8 SC-8 (1)
C8	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	No mapping
C9	Do you support the secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data (You can answer yes if your public CSP is responsible for this control and adheres by it)?	MP-1 MP-6
C10	Do you have a published procedure in data deletion controls in place after a tenant/ customer exits the service agreement?	MP-1 MP-6
Assessing Infrastructure (3.D)		
D1	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, an investigation by root cause analysis, and response to incidents?	AU-9

D2	Is logical user access to audit logs restricted to authorized personnel?	AU-9
D3	Are audit logs reviewed regularly for security events (e.g., with automated tools)?	AU-9
D4	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?	CM-6
D5	For your SaaS offering, do you provide tenants with separate environments for production and test processes?	SC-7 AC-4
D6	Do you logically segregate production and non-production environments?	SC-7 AC-4
D7	Do you restrict personnel access to all administrative consoles for systems hosting cloud virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	AC-3 AC-6 AC-6 (1) AC-6 (2) AC-6 (5) AC-6 (10) IA-5
D8	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your IT infrastructure network and systems components?	SI-3
D9	Do you have the capability to patch vulnerabilities across all of your computing devices, applications, and systems?	CM-9 RA-5 SI-2

Appendix M – Source Code and Training Data set dump

The source code and the training data set dump can be found in the CD drive within the pocket pasted inside the back cover.

This can also be accessed online by visiting https://github.com/Security-Compliance-For-SaaS-Startups/saas-security-compliance-analyzer-api