



St. Mary's ቅድስት ማርያም
University ዩኒቨርሲቲ
Committed to Excellence

ST. MARY'S UNIVERSITY
SCHOOL OF GRADUATE STUDIES
FACULTY OF INFORMATICS
DEPARTMENT OF COMPUTER SCIENCE

**PROPOSING CLOUD SECURITY FRAMEWORK
BASED ON IT GOVERNANCE**

BY

OBSA TAERA DERESSA

JUNE, 2020

ADDIS ABABA, ETHIOPIA



St. Mary's **ጳውሎስ ማርያም**
University **ዩኒቨርሲቲ**
Committed to Excellence

**Proposing Cloud Security Framework based on IT
Governance**

BY

OBSA TAERA DERESSA

A THESIS SUBMITTED TO SCHOOL OF GRADUATE STUDIES
OF ST. MARY'S UNIVERSITY IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF MASTER OF
SCIENCE IN COMPUTER SCIENCE

JUNE, 2020

ADDIS ABABA, ETHIOPIA

ACCEPTANCE

Proposing Cloud Security Framework based on IT Governance

BY

OBSA TAERA DERESSA

Accepted by the Faculty of Informatics, St. Mary's University, in partial fulfillment of the requirements for the degree of Master of Science in Computer Science.

THESIS EXAMINATION COMMITTEE:

_____	_____	_____
DEAN, GRADUATE STUDIES	SIGNATURE	DATE
<u>ASRAT MULATU (PhD)</u>	_____	_____
ADVISOR	SIGNATURE	DATE
<u>TEMTIM ASSEFA (PhD)</u>	_____	_____
EXTERNAL EXAMINER	SIGNATURE	DATE
<u>GETAHUN SEMEON (PhD)</u>	_____	_____
INTERNAL EXAMINER	SIGNATURE	DATE

DEDICATION

This work is dedicated to the love of my life Habiba Sultan whose support was priceless! Babiye my love, you are my fuel and motivation that always make me keep going forward! Babiye this is for you!

ACKNOWLEDGEMENTS

First and foremost, I would like to praise and thank the almighty God who blessed me in every step of my life and helped me finish this research. Thank you the Holy Trinity (God) for being my strength and helping me all the way up to here starting from the beginning of my life. Next I would like to give thanks to the holy virgin St. Mary, the Arch Angels St. Gabriel and St. Michael, the Martyr St. George as their hierarchies for strengthening and helping me. Thank you! Thank you! Thank you!

I would like to express my gratitude and heartfelt thanks to my advisor Dr. Asrat Mulatu. This research would not have been successfully completed without your guidance, supervision and you critically reading every part of the document quickly and replying on-time. You have supported me throughout my research with your valuable insights, knowledge and patience. You were always available to answer my questions, provided me with feedbacks and advices.

I also want to reach out and say thank you to my dearest love Habiba Sultan, who has been at my side ever since our first day. I am deeply humbled to be your life partner, lover, fiancé and husband ultimately. You are a gift from the almighty God. You have been always there through the ups and downs life was throwing and keeping me strong and pushing me to become the best version I could become. Babiye you are my soul, this thesis would not have been finished without your help and guidance. You were the editor in-chief giving me critiques and suggestions to finish the research. My love Thank you! Thank you! Thank you! for all the things you have done for me and you are doing, words cannot express what I feel about you, you just make me speechless as always! God bless you forever and ever my love!!!

Mom (Etagenehu Dagne) and Dad (Taera Deressa), thank you for all the encouragement you were giving me during my studies. I am grateful that God has given me you as my parents. May God give you many more years to live and bless you dears.

Last but not least I would like to thank family and friends who were always encouraging me in all aspects. Thank you!

DECLARATION

I, the undersigned, declare that this research work is my original work, prepared under the guidance of Dr. **Asrat Mulatu**. All sources of materials used for the thesis have been duly acknowledged. I further confirm that the research has not been submitted either in part or in full to any other higher learning institution for the purpose of earning any degree.

Obsa Taera Deressa

Full Name of Student

Student Signature

St. Mary's University,

Addis Ababa

Ethiopia

June, 2020

ENDORSEMENT

This Research has been submitted to St. Mary's University, School of Graduate Studies for examination with my approval as a university advisor.

This Research has been submitted for examination with my approval as advisor.

Asrat Mulatu (PhD)

Full Name of Advisor

Advisor Signature

St. Mary's University,

Addis Ababa,

Ethiopia

June, 2020

Abstract

Cloud computing is one of the fast growing technological phenomena being adopted by many organizations ranging from small to large and even individuals, due to the advantage that no need of infrastructure deployment needed by customers to meet their computational demands. In this research the various components of cloud computing such as service delivery models, types of cloud computing, security issues and security mechanisms used were discussed in detail. There are various security vulnerabilities and risks in the cloud environment introduced due to the fact that users do not have mechanisms of control over their confidential data in the cloud. The major security concerns raised by Cloud Service Consumers (CSCs) as seen from literatures were insufficient data security, compliance and legal issues and loss of governance on data. The aim of this research is, therefore, to provide solutions for the above mentioned security issues.

Various mechanisms were used for data gathering such as interviews and document analysis to get the full picture of the cloud security mechanisms deployed at Cloud Service Providers (CSPs) and CSCs, and analyzed them whether they address security issues and concerns faced by CSCs. Based on the data gathered it was evident that the organizations under the study that use cloud were provided with only technical security controls which are not enough to deem they are alone enough to ensure cloud security and address CSCs concerns of getting services that are secured, transparent and managed in formal manner.

Thus, in order to address these security concerns and issues, the researcher proposed a framework that encompasses end-to-end cloud environment by combining technical cloud security solutions with IT governance solutions. The proposed framework was evaluated using two methods, the first was by presenting it to the various individuals who participated in the interviews that were conducted and IT security professionals from other organizations. The other validation technique utilized was comparing the proposed framework with other cloud security frameworks. Based on the validations conducted the framework was given positive feedbacks about addressing the issues faced by CSCs and improve its adoptability.

Keywords: Cloud computing, IT governance, Transparency, Resources management, Compliance

List of Acronyms

Acronyms	Definitions
NIST	National Institute of Standards and Technology
CSPs	Cloud Service Providers
CSCs	Cloud Service Consumers
PaaS	Platform as a Service
IaaS	Infrastructure as a Service
SaaS	Software as a Service
IT	Information Technology
ITG	Information Technology Governance
EDDoS	Economic Distributed Denial of Service
DDoS	Distributed Denial of Service
ITIL	Information Technology infrastructure Library
COBIT	Control Objective for Information Technology
ROI	Return on Investment
ITIM	IT Infrastructure Management
CSA	Cloud Security Alliance
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
ITGI	IT Governance Institute
SMU	St. Mary's University
NGO	Non-governmental Organization
BYOD	Bring Your Own Device
SSL	Secure Sockets Layer
MFA	Multi-Factor Authentication
VM	Virtual Machine
HR	Human Resource
MAC	Message Authentication Code
IPS	Intrusion Prevention Systems
IDS	Intrusion Detection Systems
SLA	Service Level Agreement
KPI	Key Performance Indicator
DR	Disaster Recovery
HVAC	Heating, Ventilation and Air Conditioning
CCTV	Closed-circuit Television
HIPAA	Health Insurance Portability and Accountability Act
PCI DSS	Payment Card Industry Data Security Standard
GLBA	Gramm-Leach-Bliley Act
API	Application Programming Interface
VPN	Virtual Private Network

SVS	Service Value System
ISACA	Information Systems Audit and Control Association
ITSM	IT Service Management
CCTA	Central Computer and Telecommunications

List of Figures

Fig. 2.1: NIST Cloud Computing Architecture [7].....	6
Fig. 2.2: Example Services Available to a Cloud Consumer [7]	11
Fig. 2.3: Survey on cloud adoption security concerns [69]	15
Fig. 2.4: Domain areas of ITG [55]	18
Fig. 2.5: Evolution of IT function in organizations [21].....	19
Fig. 2.6: Overall COBIT framework [55].....	22
Fig. 2.7: ITIL service life cycle [58].....	24
Fig. 2.8: PDCA Cycle with the respective processes in ISO 27001 [59]	26
Fig. 2.9: Model for Governance of IT in ISO/IEC 38500 [61].....	29
Fig. 2.10: Components of COSO internal controls [63]	31
Fig. 2.11: CMMI Maturity Levels [66].....	33
Fig. 5.1: The Proposed Cloud Security IT Governance Framework	64

List of Tables

Table 2.1: Comparison of IT Governance frameworks	34
Table 2.2: Summary of related works.....	46

Table of Contents

ACCEPTANCE	i
DEDICATION	ii
ACKNOWLEDGEMENTS	iii
DECLARATION	iv
ENDORSEMENT	v
Abstract	vi
List of Acronyms	vii
List of Figures	viii
List of Tables	ix
Table of Contents	x
Chapter One	1
Introduction.....	1
1.1. Background	1
1.2. Statement of the Problem.....	1
1.3. Objectives of the Research.....	2
1.3.1. General Objective	2
1.3.2. Specific Objectives	2
1.4. Methodology	3
1.4.1. Literature Review.....	3
1.4.2. Tools	3
1.5. Scope and Limitations of the Research.....	3
1.6. Significance of the Research.....	4
1.7. Organization of the Rest of the Report	4

Chapter Two.....	5
Review of Literature and Related Works.....	5
2.1. Overview	5
2.2. Cloud Computing	5
2.2.1. Cloud Deployment Models	6
2.2.2. Cloud Delivery Models.....	9
2.2.3. Cloud Computing Characteristics	11
2.2.4. Security Risks in the Cloud.....	12
2.2.5. Security Measures	15
2.3. IT Governance	17
2.3.1. History of ITG.....	19
2.3.2. ITG frameworks.....	20
2.4. Related Works	36
2.5. Summary of Related Works	45
Chapter Three.....	50
Research Design and Methodology	50
3.1. Overview	50
3.2. Research Design	50
3.3. Sources of Data	51
3.4. Sample Design.....	51
3.4.1. Target Population.....	51
3.4.2. Sampling Technique	51
3.4.3. Sampling Size	52
3.5. Instruments of Data Collection.....	52
3.5.1. Interview	52

3.5.2. Document Review.....	53
3.6. Procedures for data collection	53
3.7. Method of Data Analysis.....	53
3.8. Validation	54
3.9. Ethical considerations.....	54
Chapter Four	55
Data Presentation and Analysis	55
4.1. Overview	55
4.2. Data Analysis and Presentation.....	55
4.2.1. Information Network Security Agency (INSA).....	55
4.2.2. Ministry of Innovation and Technology (MiNT).....	57
4.2.3. Debub Global Bank S.C.....	58
4.2.4. Enat Bank S.C.....	59
4.2.5. Save the Children.....	60
4.3. Data Interpretation.....	61
Chapter Five.....	63
The Proposed Framework.....	63
5.1. Overview	63
5.2. The Cloud Security IT Governance framework	63
5.3. Components of the framework	65
5.3.1. Risk Management Section	65
5.3.2. Performance Measurement Section	66
5.3.3. Resource Management Section.....	67
5.3.4. Compliance Section	68
Chapter Six.....	69

Evaluation of the Framework.....	69
6.1. Overview	69
6.2. Evaluation of the proposed framework	69
6.2.1. Evaluation from feedback.....	69
6.2.2. Evaluation by comparison.....	72
Chapter Seven	75
Conclusions, Recommendations and Future Works	75
7.1. Conclusions	75
7.2. Recommendations	76
7.3. Future Works.....	76
References.....	77
Appendices.....	80
Appendix A: - Information Sheet	80
Appendix B: - Consent Form.....	81
Appendix C: - Interview Guide.....	82
Appendix D: - Support letter.....	83
Appendix E: - Meeting Minutes	84

Chapter One

Introduction

1.1. Background

Cloud computing is one of the rapidly adopted technologies which enable customers of any business type to pay-per-use requiring no pre-existing computational infrastructure residing and owned by them. Basic definitions for cloud computing have been given by many technology groups, but in this research the definition provided by the National Institute of Standards and Technology (NIST) and the Cloud Security Alliance (CSA) is given emphasis and used. They regarded cloud computing as “a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” [1]. In other terms, cloud computing helps customers pay for the provisioned IT services on consumption, making it the fifth utility type next to electricity, water, gas and telephone services [2].

1.2. Statement of the Problem

As seen above there are many benefits for customer’s advantages to use cloud computing, but on the contrary there are also many security issues/problems weighing down the applicability of the technology. To mention some of the issues privacy, data security, compliance issues and risk of losing control [69] are the most dominant ones. These problems arise from the introduction of numerous cloud based computing services and geographically dispersed cloud service providers, sensitive information of clients are stored in remote servers and locations with the possibilities of being exposed to unauthorized parties in situations where the cloud servers storing that information are compromised.

Trust between customers and the cloud service providers is also another problem facing security concerns of cloud services, that it is directly related to the credibility and authenticity of the cloud service providers.

Thus, if security of the cloud is not robust and consistent, the flexibility and advantages of cloud computing offers less credibility. Therefore, based on the articles reviewed in the area of cloud security researches mostly focus on the separately addressing the security problems such as data privacy issues, virtualization issues, access control and identity management issues alone. However, this research suggests a possible solution and fill the security gaps of cloud computing by having a comprehensive view of the cloud ecosystem through IT governance.

1.3. Objectives of the Research

1.3.1. General Objective

The objective of this research is to deeply examining the information security problems that are found in cloud computing, propose a comprehensive security solution to minimize the security risks of cloud service providers and customers.

1.3.2. Specific Objectives

Below mentioned are the specific objectives of this research.

- ❖ Explore the overall nature of cloud computing along with its service and deployment models, and cloud computing architecture
- ❖ Through understanding of IT governance concepts
- ❖ Recognize the core security issues that prevail on cloud computing regarding its governance
- ❖ Identify research gap of cloud computing security
- ❖ Perform data collection to gather the required information
- ❖ Propose a comprehensive security solution to address the gaps of cloud security using IT governance techniques
- ❖ Evaluate the framework by validation to see it addresses security issues it was proposed to solve

1.4. Methodology

In order to achieve the fore mentioned objectives, various research methodologies were used which are depicted as follows.

1.4.1. Literature Review

Various journal articles, conference papers and books focusing on cloud computing, cloud security and IT governance were reviewed for clearly stating the current security issues of cloud computing and leveraging the advantages of IT governance to the cloud environment to propose a comprehensive cloud security framework.

1.4.2. Tools

There are different IT governance frameworks used for information security and related security matrices that were used as a reference to make the desired security framework more comprehensive and fit for purpose of cloud security. Additionally, on premise interviews, survey of work space and document analysis was conducted.

1.5. Scope and Limitations of the Research

As mentioned above there are various security issues that hinder the adoption of cloud by enterprises. This security issues can be categorized as information security, privacy, trust, authentication, identity management etc... Thus, this research focuses on solving the cloud security issue of information security and transparency. It encompasses the following listed issues: -

- ❖ The transmission of sensitive data from the user to the cloud,
- ❖ Transmission of this data from cloud server to the users and
- ❖ Storage of clients' personal sensitive data in remote cloud servers

Remaining cloud security issues are out of the scope of this research. For further studies researchers could consider the other these issues.

1.6. Significance of the Research

This research gave security solutions for the cloud using IT governance principles and theories which benefited both the cloud service providers and users on what to focus on while entering service level agreements and clearly answering questions like what the roles and responsibilities of various stakeholders of cloud are computing. The use of IT governance for the purpose of securing the cloud from its perspectives and its domain areas has not been utilized and explored. Thus this research aims to utilize the combination of these two topics that is a new finding of this research.

1.7. Organization of the Rest of the Report

The research report is composed of seven chapters. Chapter one discussed about introduction, problem statement, objectives of the research, methodology used, limitations and significance of the research which were depicted in this chapter. Then follows the chapter two which depicts the literature review and review of related works where various cloud security frameworks devised by other scholars were analyzed and critically reviewed. The next chapter addressed the methodology used to gather data, sampling techniques used, procedures of data collections. Chapter four illustrated the data gathered in the previous chapter was analyzed critically and conclusions were drawn from it. Then chapter five discussed solely about the cloud security framework devised and its various components in detail. Then next chapter the evaluation process on the proposed framework from different stakeholders participated in the research. The last chapter is composed of conclusion, recommendation, future works about ways of to enhance and improve the framework.

Chapter Two

Review of Literature and Related Works

2.1. Overview

In this chapter the researcher discussed the research domain area by exploring it deeply. The topics that were studied in this research are cloud computing, cloud security and IT governance. Finally, related researches were reviewed to get insights on how to use IT governance in securing the cloud services that are rendered to CSCs.

2.2. Cloud Computing

The idea behind using computing infrastructures as utilities was initially forecasted by John McCarthy dating back to the 1960s [49], which then was termed as cloud computing. The aforementioned definitions by NIST and CSA of cloud computing found in the previous chapter is considered throughout the research. The major advantage of cloud computing for CSCs is that it requires them no upfront infrastructure to set up and maintain, they transfer it to the CSPs along with the risks associated with it. To elaborate the cloud environment below is found the NIST cloud computing architecture depicting the essential characteristics, service models and deployment models in high-level for better understanding of requirements, characteristics and uses of the cloud.

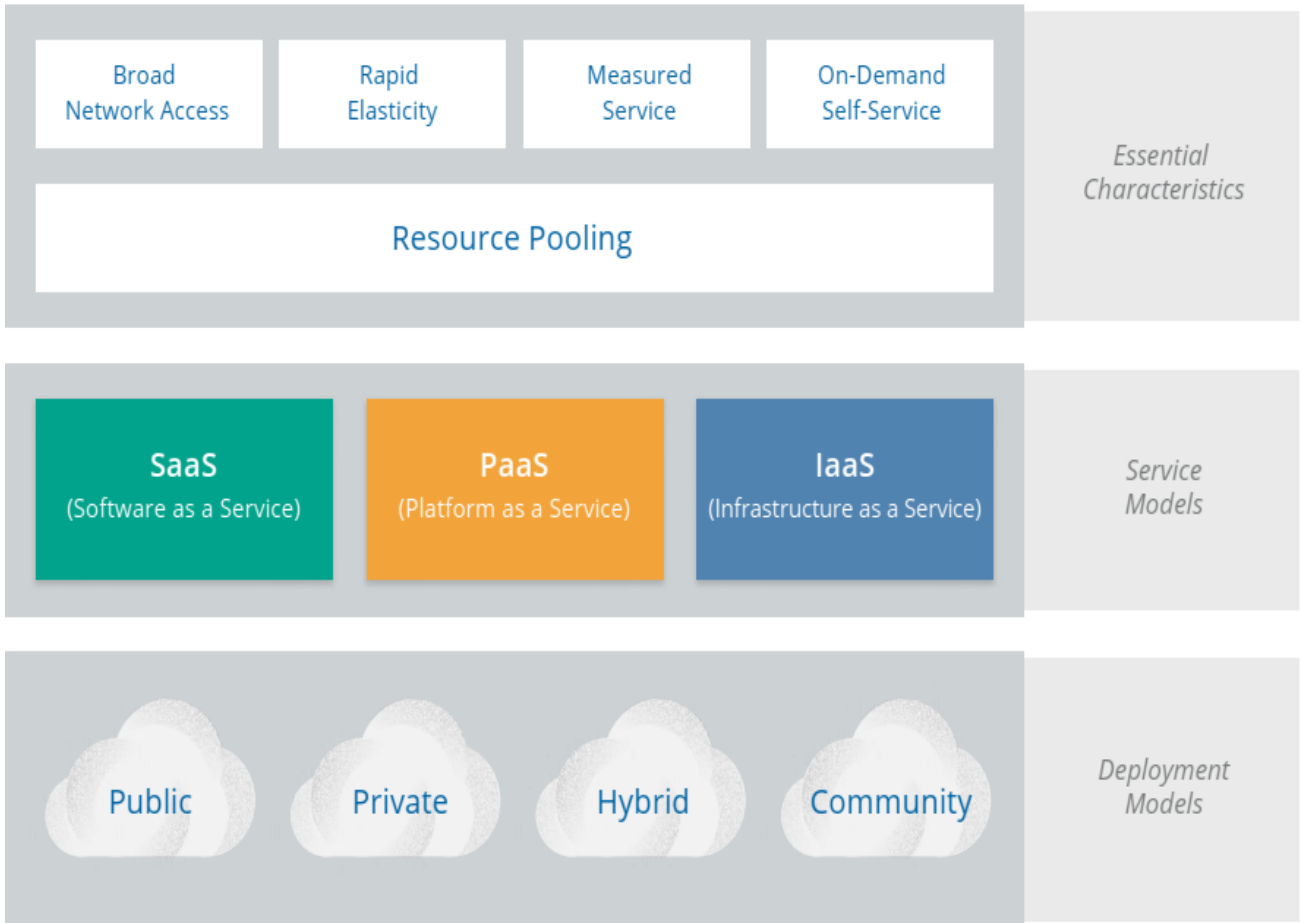


Fig. 2.1: NIST Cloud Computing Architecture [7]

2.2.1. Cloud Deployment Models

As stated in [3], there are four deployment model types namely private, public and hybrid for customers to choose based on their needs and the type of business they run. Thus, there are businesses requiring a single deployment model to be used specifically because of the sensitivity of enterprises data and highest level of demand for security is needed for the survival and business continuity of the enterprises.

2.2.1.1. Private Cloud

In this deployment model the CSP provides the necessary cloud computing resources which are dedicated only for a single organization or group of organizations that is treated as an intranet functionality [4].

The billing is usually on a subscription basis with the cloud consumers making minimum commitments for the resources and services used. The CSCs are the ones that regulate and control the architectures, processes and tools that are used in the cloud deployment, i.e. the customers demand for the use of state-of-the-art security measures for their cloud is high. Even though this deployment model has the previously mentioned advantages for security, it has its own downfalls such as high cost of implementation and management, required skills for implementation and management is high and vulnerability management difficulty are some of them.

In private cloud, cost and return on investment (ROI) are key factors and the security implementation is usually based on risk assessment and hence, the security coverage is not comprehensive [4].

2.2.1.2. Public Cloud

In a public cloud, resources are dynamically committed on a fine-grained, self-service basis over the Internet or a portal [5]. Billing is usually consumption based and is charged on a pay per use basis. In [6] the technology consulting firm Gartner has estimated market size of \$59 billion for public cloud making the use of cloud services a huge demand by various enterprises and businesses.

Due to the large number of cloud consumers and volumes of transactions in this deployment model, the CSPs employs a comprehensive and layered security systems, which can potentially provide a high degree of security due to its implement once and use multiple times model, which significantly reduces the cost of security implementation for the consumer.

Security challenges are heightened, as the resources are not committed to a single company but leveraged across multiple cloud consumers also known as multi-tenancy. This not only adds

additional burden of ensuring all applications and data accessed on the public cloud, but also the CSPs has to manage the multitude of external influences such as legislative, data protection etc. compliances that must be adhered to.

2.2.1.3. Community Cloud

This type of cloud deployment model is becoming the widely adopted deployment model [11]. The concept of community cloud originated from combining different paradigms namely Cloud Computing, Digital Ecosystems and Green Computing [50]. Community cloud can be seen as a cloud middle ground between private and public clouds, where various companies with overlapping set of needs to be met who operates by utilizing shared resources and support it. These overlapping requirements can be for organizations with joint compliance requirements, noncompetitive business goals or organizations that need to pool high-level security resources etc... The shared resources can reside in one of the members of the community founders or it may be managed by a third-party CSP. This feature makes the management of shared resources difficult and raises some other issues like latency, privacy resiliency.

In order for a cloud to be regarded as community cloud, the authors in [50] introduced some key characteristics that must be fulfilled. These are openness (creating interoperability of vendors), community (creating economic scalability by sharing within the community), graceful failures (since the cloud is not controlled by a single CSP the failure of one does not make destructive failure and minimal down time on the community), convenience and control (since it is community owned it provides democratic distributed control) and environmental sustainability (based on the demand of the community shrinking and expanding computational power making less carbon footprint emitted from underutilized servers).

2.2.1.4. Hybrid Cloud

Hybrid cloud is a deployment model that is a combination of one of the three deployment models (public, private or community) where a private cloud is linked to one or more external cloud services while being managed centrally. It provides the cloud consumers a flexible and fit-for-purpose solution with a relative ease of operations. In a research conducted by Gartner [6], hybrid cloud has been predicted to grow to \$149 billion by 2014 with a compounded annual

growth rate of 20%. The hybrid clouds have a higher degree of complexity in terms of billing and commercials compared to the other cloud deployment models. The security can be purpose-built for vulnerabilities, threats, and risks that are assessed for both parts of the hybrid cloud i.e. the private and the public cloud parts. This makes it cost-effective and targeted.

But, there are drawbacks that comes along with the use of hybrid cloud. Such as relatively complex deployment models since it incorporates heterogeneous environments, multiple orchestration, and automation tools than private and public clouds. This required additional administrative overhead, with any oversight resulting in significant risk exposure.

2.2.2. Cloud Delivery Models

The NIST cloud computing architecture states [7], the three service delivery models, which are Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS) that are the main services CSPs gives. They are briefly discussed below.

2.2.2.1. Infrastructure as a Service (IaaS)

Infrastructure as a Service is a multi-tenant cloud layer where the cloud service provider dedicated resources are only shared with contracted clients at a pay-per-use fee. This typically means that Operating System is presented to the cloud consumer. The cloud service provider's responsibility ends with the operating system. The cloud consumer builds the application without worrying about the infrastructure requirements. Security responsibility is divided equally between the CSP and CSC. The risks here are segregated and layered, making it a shared risk model.

2.2.2.2. Platform as a Service (PaaS)

NIST defines PaaS [8] as, “The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations”. It

is one of the popular delivery services where the cloud provider supplies not just the operating system but also a development stack. It is usually seen that CSPs in this model offer database and application administration along with development services. Just as in IaaS, PaaS is a pay-per-use model. This model gives a remote platform for building and customization of business processes [9].

The CSC brings the application expertise along with licenses, data, and resources, and consumes the platform shell. This model is used by consumers who either lack infrastructure skills or want to save on high capital expenditure (capex) spend required to build the infrastructure. The security responsibility weighs down to the CSP since the cloud provider supports and manages multiple layers including the infrastructure layer.

2.2.2.3. Software as a Service (SaaS)

In this service model the complete application stack is hosted by the cloud provider, who provides end-to-end resources such as application and networking. Thus, the CSP only just brings the data and business processes and utilize the services in a web-service or application oriented architecture. Such service delivery can be regarded as renting business applications [10].

SaaS is the most favorable choice where the CSCs have the necessary skills, time, or resources to setup an application ecosystem and manage it. Securing the whole services is majorly left for the CSP, whereas the consumer is only responsible for their side of transactions.

Some of the services that are given by CSPs in summarized form are depicted in the below figure.

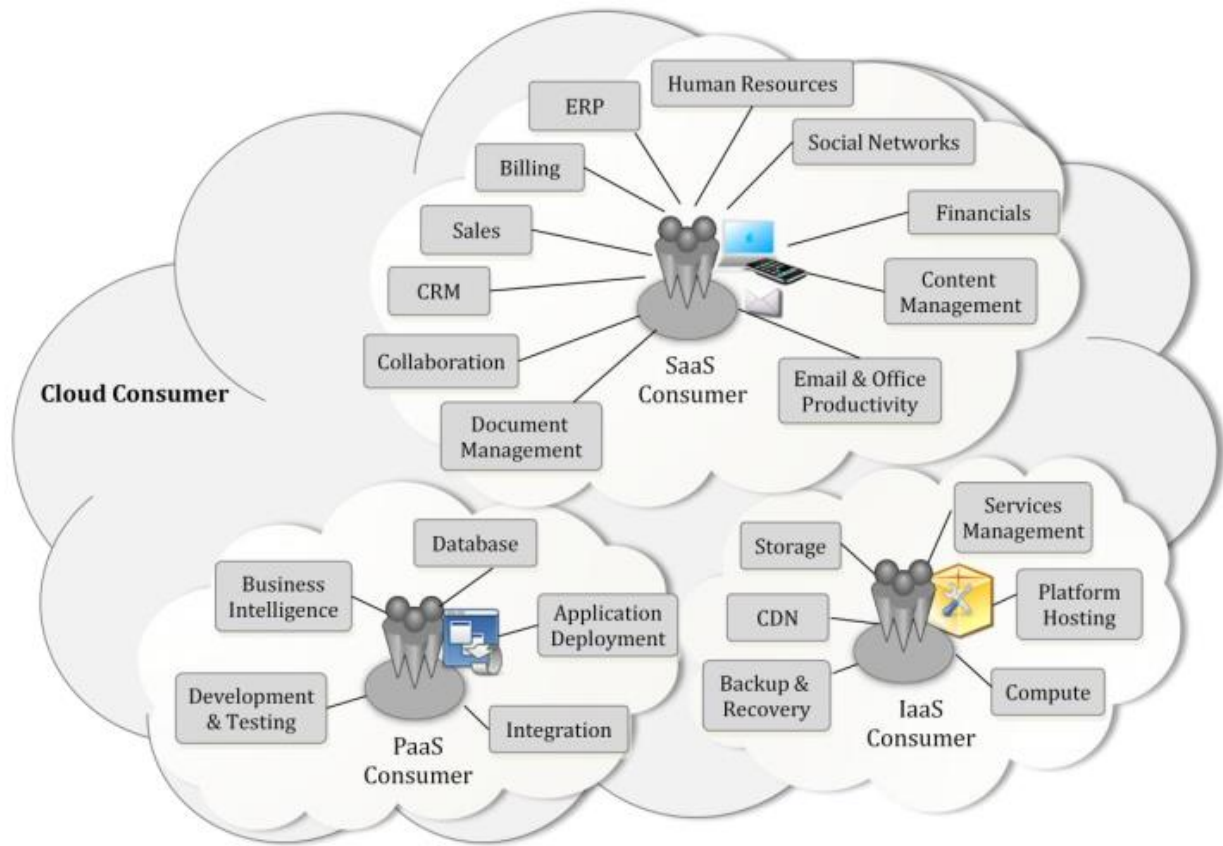


Fig. 2.2: Example Services Available to a Cloud Consumer [7]

2.2.3. Cloud Computing Characteristics

NIST [11] states the essential features that are found in cloud computing are discussed as follows:-

2.2.3.1. Resource Pooling

Computing resources like storage, network, processing and memory that consumers need are used in a multitenant model with different physical and virtual resources assigned in a way that is not in control of the CSCs. In the case of private clouds, they can achieve that by pooling the resources within the same organization.

2.2.3.2. Rapid Elasticity

This feature of cloud computing makes the resource usage increment or decrement quickly and easily based on consumer preferences. This capability emerged from the implementation of loosely coupled services where one service scales up or down the other is not affected [11].

2.2.3.3. Measured Service

The use of cloud resources by CSCs is automatically monitored, measured, controlled and reported [12]. Then consumers are billed in a transparent way that is suitable both for the service provider and the customer.

2.2.3.4. On-Demand Self-Service

This characteristic of cloud computing makes the CSCs use and make changes such as scaling up or down the resources or services which they utilize without any intervention from the CSPs [12]. This makes the time needed to disappear for various service providers to configure and maintain the cloud services/resources. The cloud consumers are given the privileges to schedule the use of cloud services like network or storage usage [11].

2.2.3.5. Broad Network Access

For effective use of cloud computing, it requires a high-band width communication links to reach the services or resources and get quality services. “One of the principal economic justifications for cloud computing is that the lowered cost of high-bandwidth network communication to the cloud provides access to a larger pool of IT resources that sustain a high level of utilization” [11].

2.2.4. Security Risks in the Cloud

Despite the tremendous business and technical advantages of using the cloud, the security and privacy concerns has been one of the major obstacles preventing its widespread adoption [12]. Especially for outsourced data services in the case of public clouds, the owners control over their data is ultimately given up to the CSPs.

Generally, these security issues arise because CSPs use firewalls and virtualizations for securing the services they provide but they are not enough to consider them as fully secured from various threats such as insiders, outsiders, other cloud tenants (non-bug free deployment) and low degree of transparency. Below discussed are some of the security risks the prevail in the cloud environment.

2.2.4.1. Outsourcing

This is a risk emerged since cloud computing gives full control of user's data to the CSPs [13]. It makes the CSCs data susceptible for abusive use by the service providers without them knowing of the incidents or events. i.e. the CSPs can do whatever they want with customer's data.

2.2.4.2. Shared Technology Vulnerabilities

This term was first coined by the Cloud Security Alliance, to describe the transferred security risks from CSPs to CSCs or vice versa that gives attackers a single point of attack since the two parties have shared technologies.

2.2.4.3. Data Breach

The movement of data from the cloud user to the cloud and from the cloud to the user has got high degree of risk in accidental, malicious and intentional data breaches.

2.2.4.4. Security Ignorant Culture of CSPs

Researches show that the majority of CSPs don't view the security of their services as one of the competitive advantage. Their only concern is that delivering their services to their customers without interruption. Furthermore, they do not consider cloud computing security is their most important responsibility and do not believe their products or services substantially protect and secure the confidential or sensitive information of their customers [14].

According to research report issued by Ponemon Institute, the majority of cloud providers believe it is their customer's responsibility to secure the cloud and not their responsibility at all. They also say their systems and applications are not always evaluated for security threats prior to deployment to customers [14].

2.2.4.5. Abusive Use

Certain features of cloud computing can be taken for granted and used for malicious attack purposes. A typical example of such attack is using a trial period of use for a cloud service and launch zombie and DDoS attacks.

2.2.4.6. eDDoS

This type of denial of service attack is caused when a malicious activity is detected or known to be on progress but the CSPs being attacked does not stop services since the customers are utilizing their other services. In order to balance the resource utilization by genuine customers and eDDoS, the CSPs incur a huge amount of fortune by adding the necessary resources for the service continual and quality of service [12].

In [69] the researcher undertook a survey to identify the causes which are discouraging users from adopting cloud computing and gain which factors were the causes. The top three most security concerns are insufficient data security/availability, open compliance or legal issues and losing governance over ones owns data which are the core areas that this research tries to overcome and provide secured, transparent and adoptable cloud for CSCs.

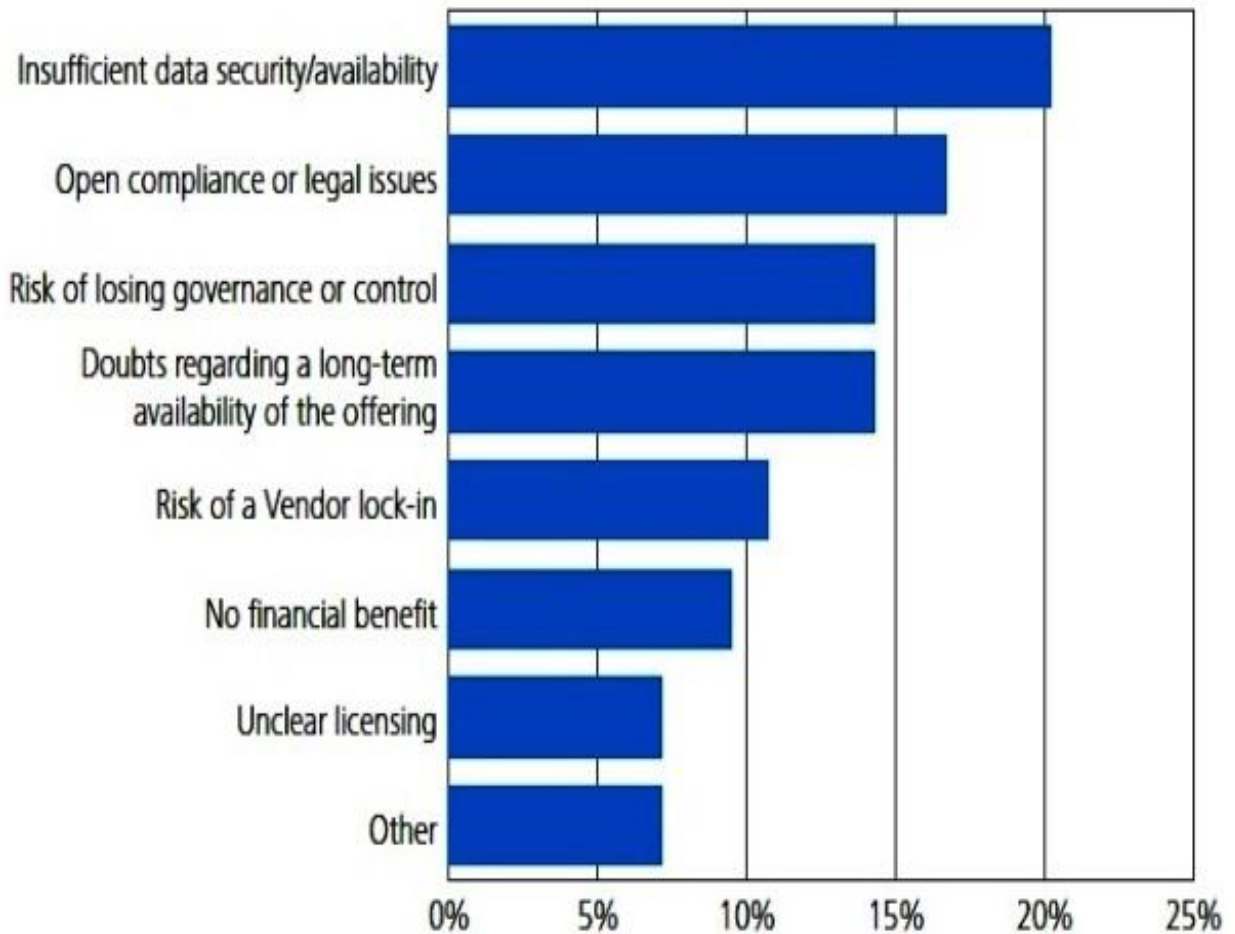


Fig. 2.3: Survey on cloud adoption security concerns [69]

2.2.5. Security Measures

In order to prevent the security risks that are found in cloud computing various security mechanisms are used. Security best practices are used for ensuring the security of services and for gaining the trust of cloud consumers. They range from physical datacenter security to specific and sophisticated API security.

2.2.5.1. Certification and Accreditation

There are various certificates that the cloud service providers can be certified to make their services secure and trustworthy. Certifications in SAS70 type II audit, ISO 27001, PCIDSS level 1, FISMA moderate level are some of the well-known certificates that CSPs get certified in to win over and get more customers. The certification authorities vouch for the services that the CSPs provide.

2.2.5.2. End-to-End Encryption

The use of strong encryption using larger number bit-keys for securing the data integrity is also another way to secure the services given by the CSPs. Encryption algorithms such as AES, DES with common PKI infrastructure can be utilized for securing the CSCs data at the transmission from them to cloud servers and from the servers back to the users.

2.2.5.3. Malicious Activity Scanning

Active monitoring and vulnerability scanning of shared resources should be performed in order to identify malicious activities and mitigate the risk of damage that could be caused. Though the use of end-to-end encryption makes it hard to trace malicious activities through firewalls, IPS and IDS.

2.2.5.4. Physical Security

The physical security of the datacenters that stores the private sensitive customer data mainly resides on the hands of the CSPs. Thus, building these datacenters in industry standards and well accepted way is the responsibility of the cloud provider. On the contrary network and application level security is mostly handled by the CSCs varying on the type of service they are using whether IaaS, PaaS or SaaS.

2.2.5.5. Data Protection at Transit and Storage

Use SSL at the cloud servers for securing private users data. A certificate verified by an authentic certificate authority like COMODO or VeriSign is used to authenticate server with the browser. Uploading private sensitive data encrypted using open source and free encryption tools.

In the figure above a survey conducted on the adoption of cloud is depicted, where it is shown that the top 3 issues that are hindering the use of cloud are data security, compliance or legal issues and risk of losing governance and control.

2.3. IT Governance

The concept of IT Governance is found under the umbrella of Corporate Governance where IT resources are aligned and enhancers for the achievement of corporate strategy [19]. IT governance in short ITG, is a system which encompasses huge scopes such as leadership, organization and decision rights, scalable processes and enabling technologies [15], by assigning roles and responsibilities that must be adhered for the effective and efficient use of IT infrastructures in organizations. In [16], describes ITG as the way enterprises lead their information technology infrastructures. In [17], ITG is regarded “specifying the decision rights and accountability framework to encourage the desirable behavior in the use of IT”. Different scholars and institutions have given various definitions for the term ITG but there is no one definition that is settled up on as the final definition and meaning of ITG [68]. One of the goal that ITG achieves is to align IT with core business, making IT an enabler and success factor for organizations [18].

As stated in [52], the benefit of IT governance for businesses growth, sustainability and support is very critical. Thus, organizations should adopt and use an IT governance mechanism for operating its IT infrastructures and services.

There are five domains of ITG where the governance of IT should focus which are put forth by ITGI, they are strategic alignment, value delivery, risk management, resource allocation and performance management [55]. These domains are discussed briefly below

- **Strategic alignment** – this domain specifies that IT governance strategies and plans should be aligned with organization’s strategy i.e. ITG strategies must be derived from the corporate strategy or else it wouldn’t deliver the intended results.
- **Value delivery** – the advantage that arises from using ITG is seen by the value that it adds to the organization seen in every aspects of business processes in order to maximize profits.
- **Risk management** – organizational risks that are faced are managed and minimized to the level that is acceptable through utilizing IT governance, thus attaining business continuity and resilience.
- **Resource management** – unwanted and excessive resource allocation and utilization are averted by the use of IT governance. Thus, optimal allocation, investment and use of IT resources is achieved.
- **Performance management** – through the use of ITG organizations can measure their performance of IT usage and provide future directions on how to enhance this performance.

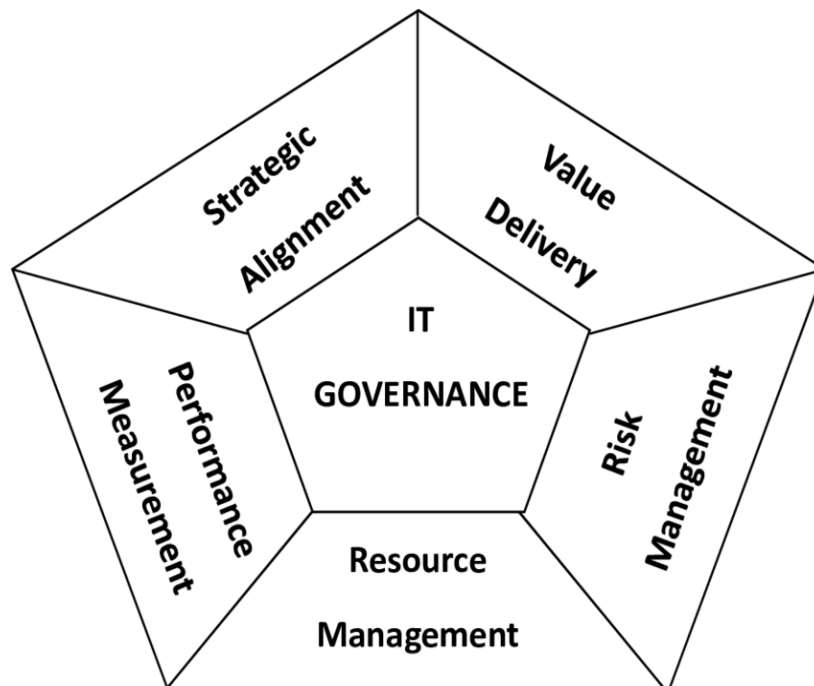


Fig. 2.4: Domain areas of ITG [55]

2.3.1. History of ITG

The use of IT is now one of the mandatory issues for the survival and business continuity of organizations. Before reaching this stage it went through a lot of challenges and changes. At the beginning IT was regarded as a technology provider for the organization and currently it is a strategic business partner for organizations [20].

As mentioned in [21], IT went through three phases. In the foundation phase the effective management of IT infrastructure was the main motive and drive for organization while utilizing IT known as IT infrastructure management (ITIM). At the next phase provision of high-class IT services (IT service provider) for sensible time and cost became the concern. Currently, IT is a strategic partner for organizations. This means that IT not only supports the business but also empowers as well as drives the business strategies and objectives to be achieved [22].

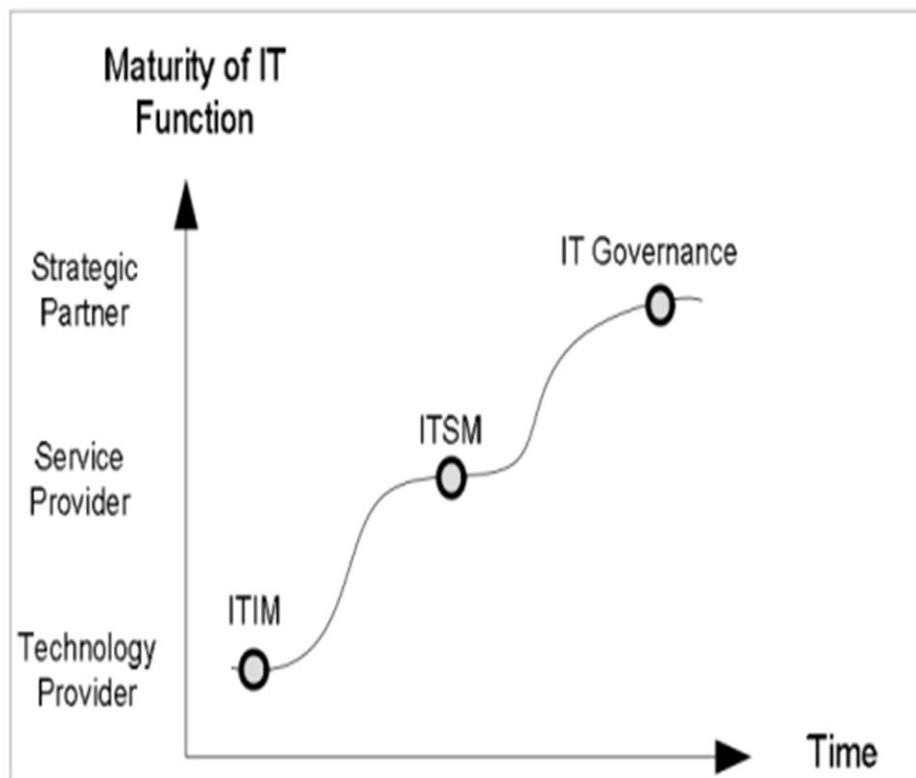


Fig. 2.5: Evolution of IT function in organizations [21]

2.3.2. ITG frameworks

IT Governance frameworks are used by organizations to enhance IT operations with IT alignment, compliance, service management, process quality and security management [22]. There are different IT governance frameworks that are developed by various institutions and standardization organizations for various purposes. They are discussed in the following sub-sections.

2.3.2.1. COBIT

COBIT (Control Objectives for Information and related Technologies) is an ITG framework that originated in 1996 [23], is a set of best practices for IT management. It was developed initially by Information Systems Audit and Control Association (ISACA) and now currently maintained by IT Governance Institute (ITGI). This standard has got six main components and is usable in 160 countries around the world [24]. The current version is COBIT is COBIT 5, which is the published in 2012. There are 5 basic principles behind the development of COBIT 5 which are meeting stakeholder needs (support business value creation through IT by attaining organizational objectives), covering the enterprise end-to-end (address all functions and processes of an organization by making sure that IT-related governance and management enablers touch the whole organization), applying a single integrated framework (easily aligns with other standards or frameworks making it mutually beneficial as one), enabling holistic approach (takes into account various interacting components internal and external) and separating governance from management (where governance is setting direction, monitoring performance and compliance against organizational objectives while management is planning, building, running and monitoring activities set by a governing body). These principles enable the framework to archive its objectives in the governance and management of IT infrastructures [51], the processes within the governance and management bodies are clearly and distinctly formulated by separating these two bodies.

Additionally, COBIT 5 defines enablers for the framework to achieve organization's objectives which are: -

- **principles, policies and frameworks** (provide practical guidance for operational activities management)
- **processes** (activities and practices to achieve organizational objectives that support IT-related goals)
- **organizational structures** (determines the major decision makers in an organization)
- **culture, ethics and behavior** (used to enhance governance and management activities)
- **information** (needed for the smooth operation of organization)
- **services, infrastructure and applications** (the infrastructure, technology and applications for information technology processing and services)
- **peoples, skills and competencies** (needed for successful application of activities and processes)

There are 37 IT processes which are structured to present the necessary information for bridging the gap between business risks, control needs and a detailed 300 IT controls in COBIT which are derived from the 5 principles which form the basis for the implementation of the framework [53]. All the above benefits as well as performance measurement mechanisms like Key Performance Indicators (KPIs), Critical Success Factors (CSFs), Maturity Model (CMM) and Key Goal Indicators are present in order for evaluating the frameworks performance. The general framework of COBIT that gives an overall view of how it works is depicted below.

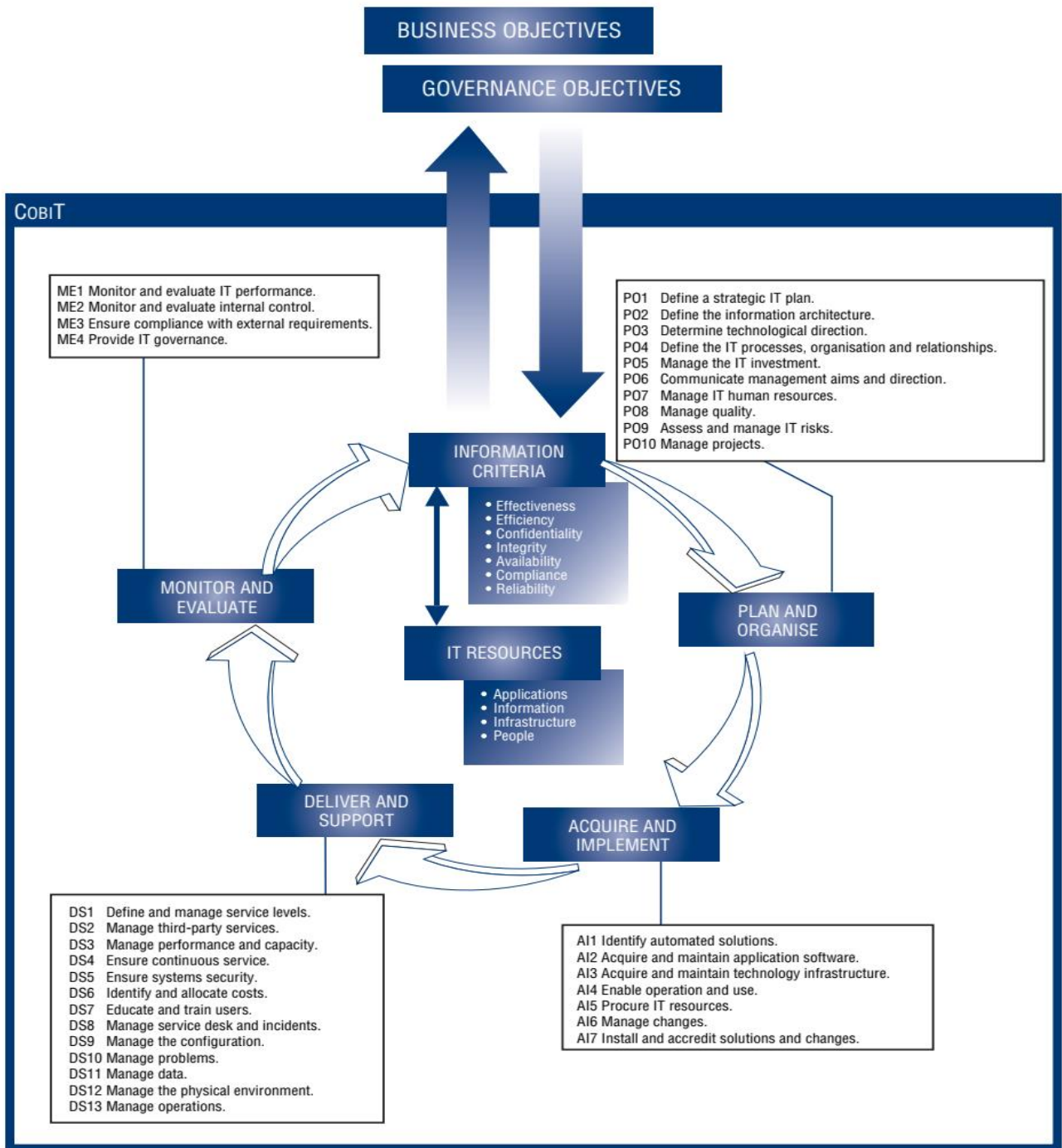


Fig. 2.6: Overall COBIT framework [55]

2.3.2.2. ITIL

Information Technology Infrastructure Library (ITIL) is a framework initially developed by Central Computer and Telecommunications (CCTA) which was later merged to the Agency Office of Government Commerce (OGC) of the Great Britain consisting of best practices for IT service management (ITSM) and service delivery by aligning them with business needs. Since 2013 the ownership of ITIL is managed by AXELOS which is a joint venture of Capita and the UK Cabinet Office [56].

A service in ITIL is defined as “A means of enabling value co-creation by facilitating outcomes that customers want to achieve, without the customer having to manage specific costs and risks”. The current version of ITIL is ITIL v4 released in 2019 which updates its predecessor ITIL 2011 [56].

ITIL have got 5 huge volumes in its 2011 version covering the different stages of ITSM namely ITIL Service Strategy (SS), ITIL Service Design, ITIL Service Transition, ITIL Service Operation and ITIL Continual Service Improvement [24]. These stages were based over the famous Edwards Deming’s plan-do-check-act (Deming or PCDA cycle), a process model for managing operations.

ITIL 4 consists of two key portions the ITIL Service Value System (SVS) and the four dimensions’ model. First explored is ITIL SVS, which is composed of 5 core components namely

- ITIL service value chain (comprised of 6 activities required in service management these are planning, improving, engaging, design and transition, obtaining or building, and deliver and support),
- ITIL practices (general service practices, service management practices and technical management practices which are 14, 17 and 3 practices respectively that were processes in its earlier version),
- ITIL guiding principles (which are the basis for ITIL like value generation, improve capabilities and end-to-end responsibility), governance (performs actions like giving directions and controlling processes are being implemented as directed) and

- continual improvement (covers the operational practices in how to improve them and reach a desired state).

The second portion of ITIL 4 introduces a model that provides a holistic approach in the arena of service management. The model is comprised of 4 elements that the SVS must take into account are listed as follows

- organizations and people (denotes the people found in organizations and the structure of the organization)
- information and technology (states that technology drives the process of service management and supports information by protecting it)
- partners and suppliers (denotes that the communication and connection with other stakeholders impacts the performance of service delivery thus must be taken in to account accordingly)
- volume streams and processes (are set of work flows or steps that organizations undertake to render services in order to gain some value)

The life cycle of ITIL 4 is depicted below showing an overall view on how to excel at ITSM.

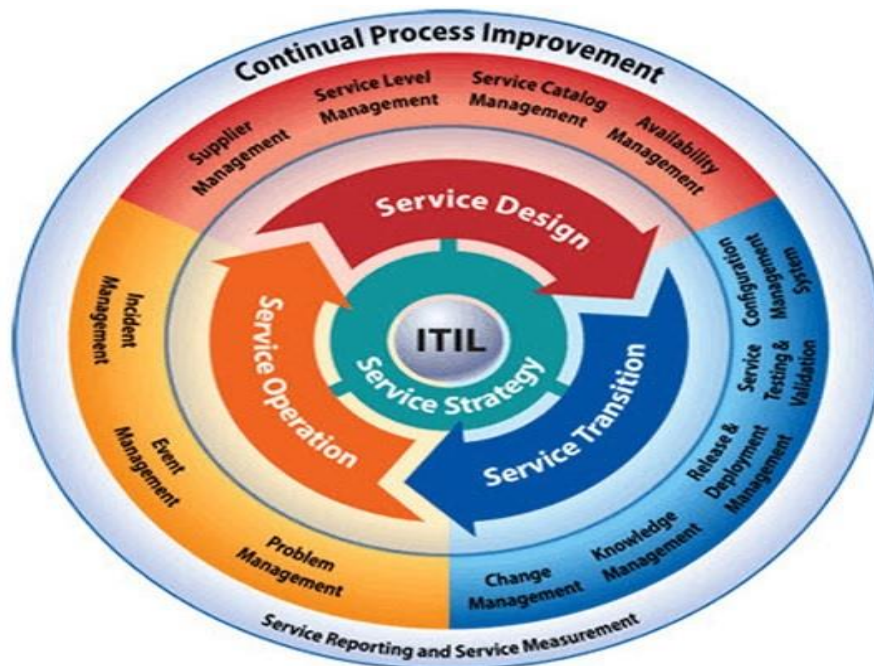


Fig. 2.7: ITIL service life cycle [58]

2.3.2.3. ISO/IEC 27001

ISO/IEC 27001 is a standard formulated by two organizations International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) created as Joint Technical Committee (JTC) 1 and Subcommittee (SC) 27 [54]. This standard is one of the well-known and globally accepted standard for ITG, with the scope of information security at its core [24]. It was formerly known as ISO 17799:2005. The current version of the standard was published in 2013. Generally, 84% of the world countries use various ISO standards, making it the most widely used standardization organization. There are a series of standards in this group of standards known as the 27000 series (27k series) all focusing also on information security.

ISO/IEC 27001 is developed with the main purpose for specifying the necessary requirements for the establishment, implementing, maintenance and continual improvement an information security management system (ISMS) for an organization. An ISMS when implemented correctly actualizes confidentiality, integrity and availability of organizational information through risk management processes by being embedded in an organization's business processes and becoming part of an organization's structure. It is structured in the form of clauses where each clause represents a set of requirements which are briefly mentioned below.

- **understanding the context of the organization** – know internal and external environment, stakeholders with their needs and expectations, and determine the scope of the ISMS.
- **leadership and commitment** – top management should check, monitor, control and ensure whether security objectives are aligned with organizational objectives, they are yielding the expected outcomes, implement security policy.
- **planning** – procedures to be taken to address risks and opportunities based up on information risk assessment results, information risk treatment methods, ...
- **support** – support the process of ISMS establishment through resource allocation, assignment of qualified and competent people with the right competency set, open communication flow between ISMS components and making documentation of the whole process available for the dedicated persons.

- **operation** – perform the works needed to address information security objectives through careful planning, implementation and controlling of processes required
- **performance evaluation** – the ISMS performance should be measured by internal audit and top management review.
- **continual improvement** – since organizations operate in a dynamic environment the ISMS should take into consideration this operational environment and take proactive measures.

Additionally, the requirements along with the controls i.e. security measures that organizations should put in place are also attached at the end of the standard clause-by-clause. Originally the framework was based on the Deming cycle in order to address security issues of organizations.

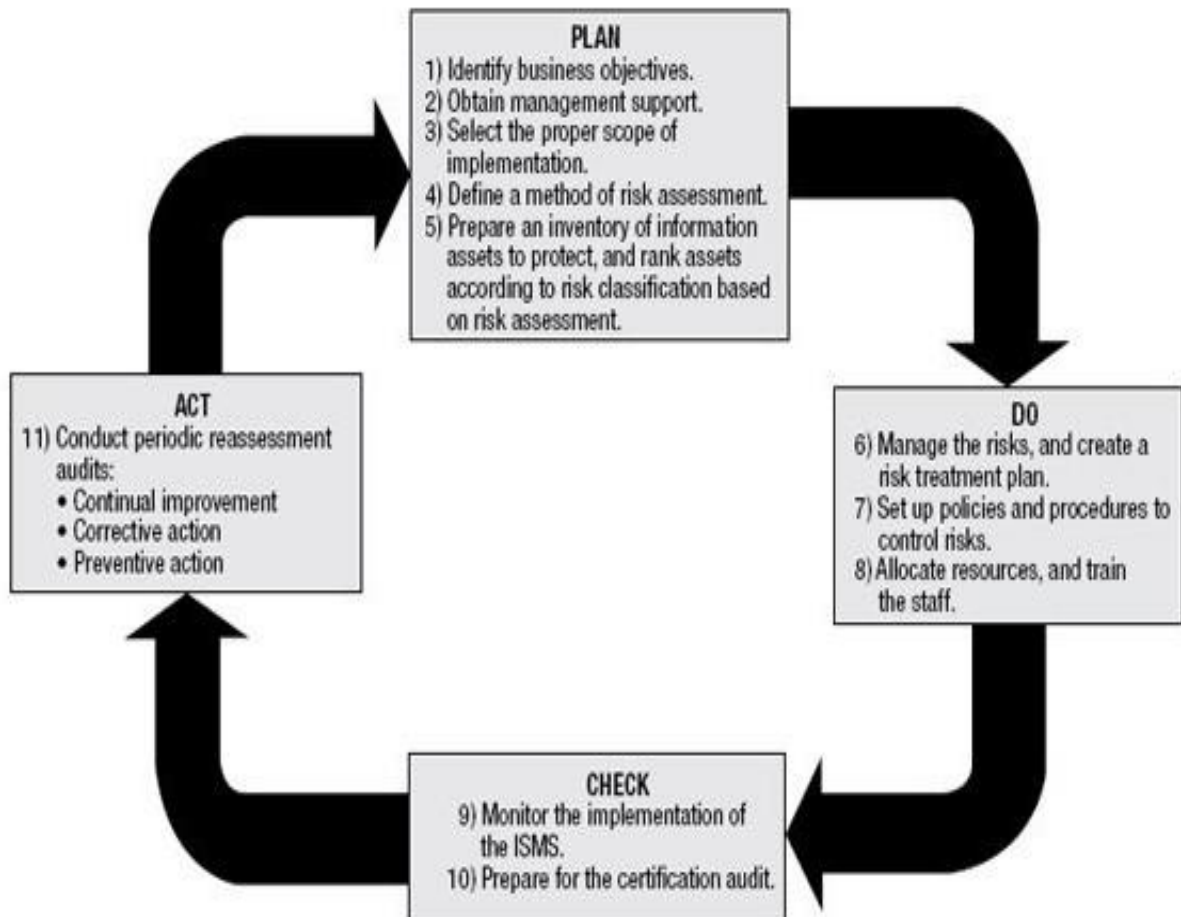


Fig. 2.8: PDCA Cycle with the respective processes in ISO 27001 [59]

2.3.2.4. ISAE 3402

ISAE 3402 in short for International Standard on Assurance Engagements 3402 is a standard for auditing service providers which was launched in 2011 by International Auditing and Assurance Standards Board (IAASB) [62]. This standard covers on how organizations should assure their services of compliance to their customers and users. This standard can be used as tool for auditing service provisions in order to gain confidence from customers. Through the use of ISAE 3402 the organizations can audit underlying governance frameworks such as COBIT to be more efficient and suitable to their organization. It provides two types of Service Organization Control (SOC) reports Type I and Type II that are a means of assurance for customers that needs to know the state of the services they are using in terms of financial values; additionally, it also helps for performing audit operations on systems and services.

- **Type I report** – gives a birds-eye-view of the overall controls in place at the organization. A snapshot at a given time or moment on where controls are situated and how much of the organization they cover, this report can be used as quick reference.
- **Type II report** – shows the management of controls throughout a specific period of time like 6 months or 1 year. The details include how systems were designed and implemented, keep track of changes made to systems, risks that emerged, controls that were used/applied in that specific period of time. The auditor assesses the aforementioned aspects are dealt with or not and gives recommendations based on findings.

2.3.2.5. ISO/IEC 38500

This is an international standard formulated by the joint task force of ISO/IEC a framework for the provision of effective governance of IT in organizations by taking into account the legal, regulatory and ethical obligations that must be adhered by the top-management organ. Initially it was based on the standard AS8015 (Australian Standard for Corporate Governance of Information and Communication Technology) published in 2005. After 3 years in 2008 by a joint task committee from Standards Australia and experts across the globe made it an international standard known as ISO/IEC 38500:2008 (Corporate Governance of IT). In the year 2015, the standard was updated by considering the evolution of IT to suite current trends and aspects by

widening its applicability, and it was renamed as Governance of IT for the Organization. ISO/IEC 38500 states 6 principles that are mandatory to the governance of IT in an organization, they are depicted below

- **Responsibility** – it provides individuals of the organization to accept and understand their responsibilities and their authority for making decisions regarding IT.
- **Strategy** – the IT strategy should be based on the organization’s strategy and makes sure to achieve it.
- **Acquisition** – the acquisitions of IT infrastructures should be based on analysis to balance benefits, opportunities, costs and risks.
- **Performance** – IT makes business requirements to be met with quality.
- **Conformance** – IT makes sure mandatory regulations and legislations are met and also enforced through policies and practices.
- **Human behavior** – people in the organizations are given of top concern so their needs are to be addressed in the IT policies and practices.

The ITG model of ISO/IEC 38500 is comprised of three major activities, which are Evaluate, Direct and Measure. These activities are performed by the top-management of the organization in order to drive IT governance of the organization. The model is found below

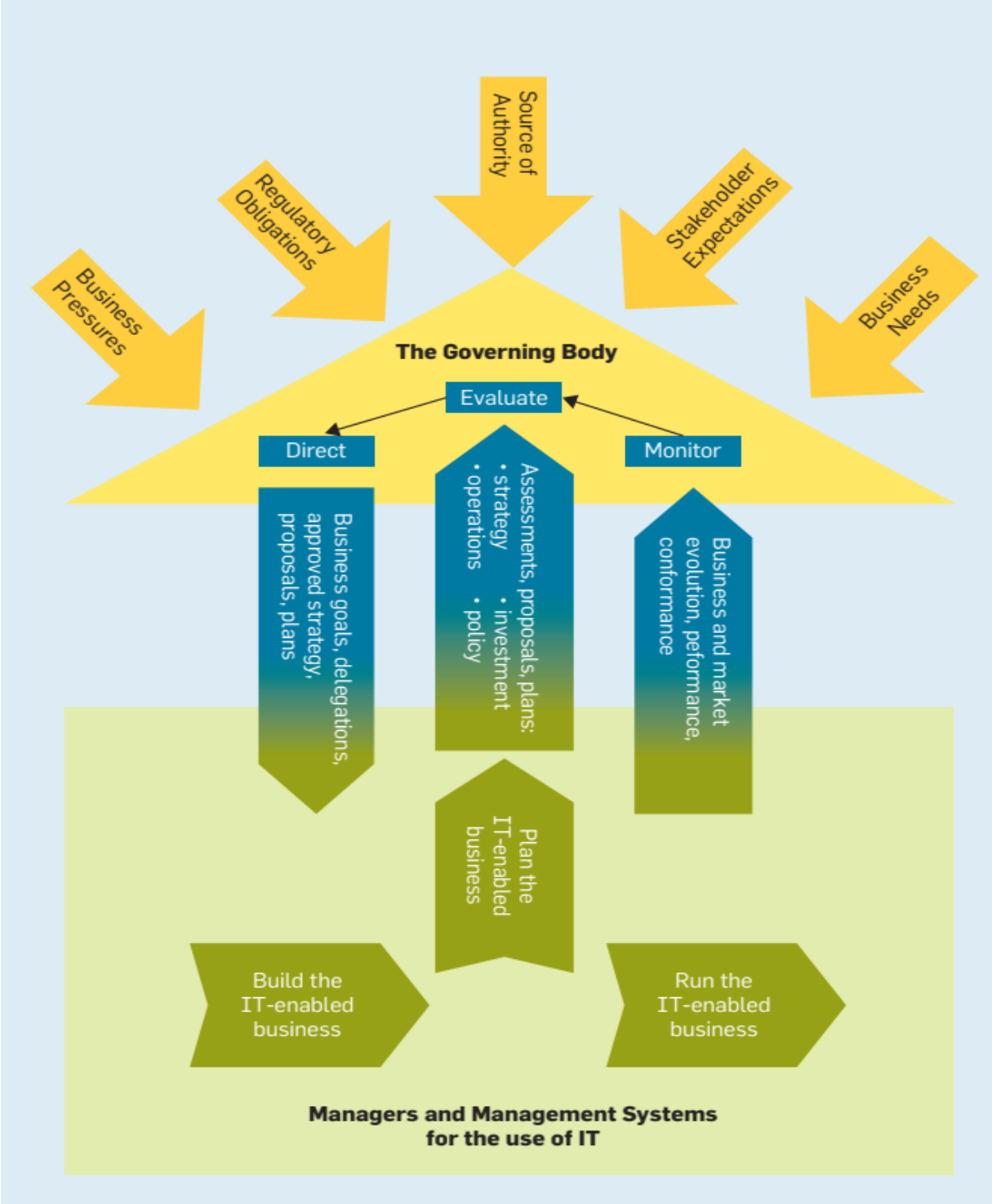


Fig. 2.9: Model for Governance of IT in ISO/IEC 38500 [61]

2.3.2.6. ISO/IEC 20000

It is the pioneer of ITSM standards that was developed by ISO/IEC Joint Task Committee (JTC) 1 and Subcommittee (SC) 7 in 2005. ISO/IEC 20000 was revised two times in 2011 and 2018 [57] to suite the dynamic nature of IT services. It was initially based on the standard BS 15000 of BSI (British Standards Institution) which was first issued in the year 2000 mainly focusing on ensuring the quality of IT services [60]. This standard has got 2 main parts namely ISO/IEC 20000-1 and ISO/IEC 20000-2 which discusses specifications for IT service management and IT service management code of practice respectively, in addition to that there are supporting documents from BSI that can be used to assist organizations for its adoption. Additionally, ISO/IEC 20000-1 derives its principles from another ISO standard 9000 which is used for quality management.

The first part illustrates the minimum requirements for organizations to establish, implement, maintain and continually improve a Service Management System (SMS), and the requirements that they should fulfill in order to be certified. Whereas the second part illustrates the best practices, guidelines and recommendations that are demonstrated to provide more efficient and effective service using IT resources that organizations use in order to achieve their goals.

Similar to the ISO/IEC 27001 standard, this standard also uses the afore mentioned Plan-Do-Check-Act cycle also known as the Deming cycle for the continuous management and improvement of SMS.

2.3.2.7. COSO

The Committee of Sponsoring Organizations of the Tredway Commission (COSO) framework is an Internal Control – Integrated framework set up by five organizations of America in the year 1992. The organizations that brought forth COSO were the Institute of Management Accountants (IMA), the American Accounting Association (AAA), the American Institute of Public Accountants (AICPA), the Institutes of Internal Auditor (IIA) and Financial Executives International (FEI) [63]. COSO can be used for various purposes by organizations in designing, implementing, conducting internal control and assessing the internal controls where organizations put in place for smooth work flow, compliance and regulation purposes. An

internal control is defined in [63] as “Internal control is a process, effected by an entity’s board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance”.

The framework is composed of 5 components which are listed below and briefly discussed as follows along with the diagram

- **Control environment** – it lays the background for the remaining components to be carried out. The overall setup of the organization is studied here such as the management’s operation style, business processes, management processes and other mandatory aspects.
- **Risk assessment** – the various risks that exist within the organization which are in the way of meeting organizational objectives should be identified and managed. Thus, risks must be assessed to give direction on how to manage and mitigate them.
- **Control activities** – these are the policies and procedures utilized for addressing the identified risks in the previous component. They give assurance on the implementation of management directives set at the organization.
- **Information and communication** – information flow and communication within organization should be effective in order to ensure the control activities are communicated to stakeholders and other parties.
- **Monitoring** – assessment of systems performance must be conducted in order to take corrective measures on deficiencies of controls and improve them.

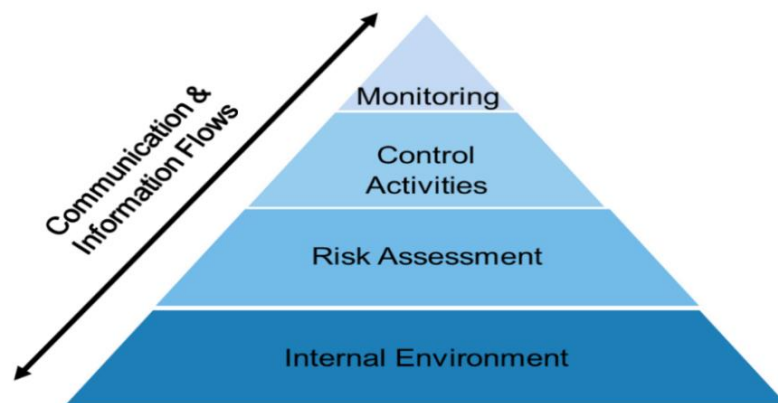


Fig. 2.10: Components of COSO internal controls [63]

2.3.2.8. CMMI

Capability Maturity Model Integration in short CMMI was a project initiated by the Software Engineering Institute (SEI) of Carnegie Mellon University used for the integration of software production, it originated in 1993 formerly known as just CMM [65]. The major use for CMM was in software engineering where software projects were failing highly at that time and in order to increase their success rate. It is based on process improvement and the paths that must be taken in order to reach the desired state in another terms organizational business objectives or goals. There are 5 stages which are hierarchical representations for process improvement of CMMI namely initial, managed, defined, quantitatively managed and optimized. Organizations of any type or size can leverage from using this model in their services and processes improvement activities [66].

The current version of CMMI is v2.0 which came out in 2018 updating its predecessor v1.3 that was published 8 years prior [64]. There are three focus areas of CMMI where it can be used for products or service development, service establishment and management, and product or service acquisition which are merged into one model. CMMI can be used for security purposes in two ways security management (manage services security) and, security design and development (manage the designing and development of software in a secure manner).

The hierarchy of CMMI v2.0 is put forth as follows Model → Categories → Capability Areas → Practice Areas → Practice Groups → Practices [64]. There are 4 categories namely doing, managing, enabling and improving in CMMI v2.0 model, and within these categories there are 12 capability areas that should be covered. In order for the capabilities to be reached there are 25 practice areas that should be worked on. The hierarchy model is briefly shown below with the categories along with their underlying capability areas.

- Doing
 - Ensuring Quality
 - Engineering and Development Products
 - Delivering and Managing Services
 - Selecting and Managing Suppliers

- Managing
 - Planning and Managing Work
 - Managing Business Resilience
 - Managing the Workforce
- Enabling
 - Supporting Implementation
 - Safety
 - Security
- Improving
 - Building and Sustaining Capability
 - Improving Performance

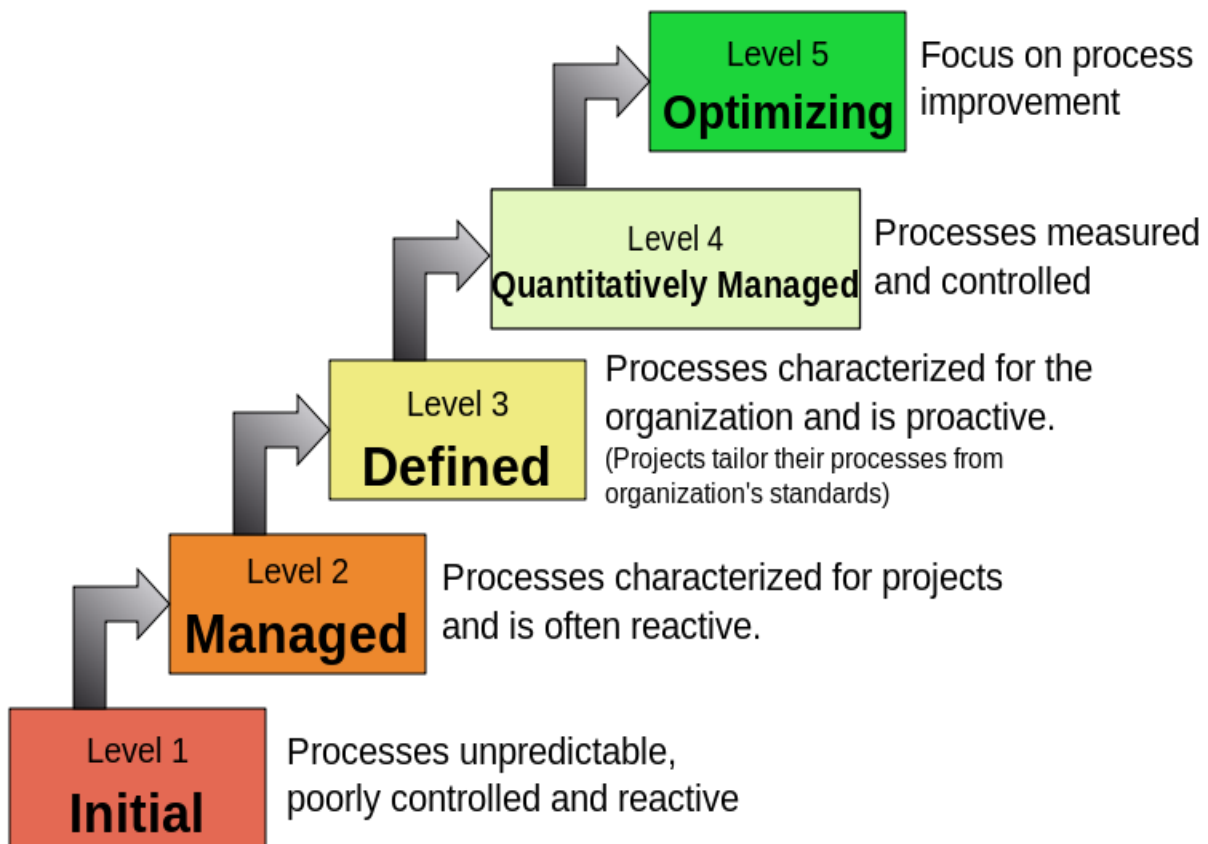


Fig. 2.11: CMMI Maturity Levels [66]

2.3.2.9. Analysis of IT Governance Frameworks

The aforementioned IT Governance frameworks are compared based on the focus areas they cover i.e. the focus areas which the frameworks take into account in order to solve issues related to IT Governance and cloud security such as service management, security management, cloud security and organizational coverage.

Table 2.1: Comparison of IT Governance frameworks

Frameworks	Comparison criteria (focus area)					
	Organizational coverage (end-to-end)	Security management	Service level management	Cloud security	ICT infrastructure management	Financial management
COBIT	X	X	X		X	X
ITIL	X	X	X		X	X
ISO/IEC 27001	X	X	X		X	X
ISAE 3402	X	X			X	X
ISO/IEC 38500	X	X	X		X	X
ISO/IEC 20000	X	X	X		X	X
COSO	X	X			X	X
CMMI	X				X	X

The above table is a summarized comparison between the various IT Governance frameworks available. The criteria for the comparison tried to cover the necessary aspects of the frameworks for this research. Thus, based on the comparison all the frameworks under the study takes into account the organization end-to-end and as a single entity meaning that the business processes (work flows), organizational structures, procedures and other aspects of the organization seen as a whole.

Another criterion used was security management in which the IT Governance frameworks improve security on the services and processes they use in order for them to achieve their goals and objectives. The only ITG framework that does not have the feature of security management is CMMI, while the others address this issue.

The third criterion used was service level management, in this category the services that are given to customers are managed by the contracts signed by both the service providers and consumers. It is used as a guiding document between these two parties on any issues that arise and how to solve them. Only the four (COBIT, ITIL, ISO/IEC 38500 and ISO/IEC 20000) out of the eight ITG frameworks help in the management of services.

Since one of the domain area of IT Governance is value delivery, organizations which use it have advantage on financial management (which is another criterion used for comparing the frameworks) of IT infrastructures and assets possible which adds to their profit. As seen above in the table all the frameworks under this study achieve that.

ICT infrastructure management was also another criterion for comparison since the governance of IT also includes the IT infrastructures implemented by organizations to achieve their goals and objectives. Thus, all the ITG frameworks are fit for the purpose of ICT infrastructure management.

Finally, as seen in the above table the IT Governance frameworks that are freely and commercially available provide an immense benefit for organizations be it service providers or service consumers of various types of IT services. Although these frameworks provide many benefits, they do not address the overarching security challenges and issues that prevail in the cloud computing environment.

2.4. Related Works

In this subtopic the topics discussed are cloud computing security solutions and frameworks that have been devised by various scholars in order to make it more secured and have a wider adoption by customers. Most of the security solutions are mainly focusing on the technical aspects of the cloud computing that address specific security issues such as encryption and firewall. Our framework is holistic and novel by trying to solve these issues all at once by taking into account the technical and non-technical (policies, standards, governance, etc...) aspects of cloud security solutions. In order to make it organized and easy to understand the security solutions are classified based on two parameters cloud storage solutions and data security solutions in transit i.e. from CSPs to CSCs and vice versa and discussed them as follows.

S. K. Sood in [25] proposed a combination Message Authentication Code (MAC), classification and Index and Encryption) approach to securing data in cloud, consisting of two stages. The author regarded cloud as it is composed of three entities, which are the cloud, cloud data owner and cloud user. The first stage is concerned about how data is securely stored in cloud. Initially, the CSCs determines the sensitivity based on confidentiality, integrity and availability of own data by entering values for each of the security properties of the data to be stored. Then the sensitivity Rating (SR) is computed by the algorithm which determines where that data is going to reside and be retrieved from i.e. from a segregated portions of the cloud in top down manner as private, public, or owner's limited access where access is allowed from bottom up but not the other way. Before the classified data is stored in the cloud it is encrypted in SSL 128bit and indexed to make searching and retrieving purposes easy and quick which is also encrypted using SSL and Message Authentication Code is appended in it to verify any changes have been made to the originally stored data. The second stage is the retrieval of the securely stored data to CSCs. The user initially initiates by requesting for a user name and password from the CSPs, where that request and information is stored in the cloud. Then the CSC requests the cloud for a file that is stored in a segregated format, if the requested file is in the public section then no authentication is required and the user gets the data but if the requested information is found in the private or owner's limited access section then authentication is mandatory in order to obtain data. Consequently, the cloud checks for the user name and password of the requester is registered or

not. Following that the user sends his/her password for the data owner in order to be authenticated if answered the security questions of the owner. If answered correctly the owner sends his/her digital signature along with the user identity to the cloud for one-time data access only. The users then send search keywords for the data to be searched, where the cloud initially verifies the digital signature and process the search request. Entries found based on the keywords are forwarded from the cloud to the user in an encrypted format as stored, which leaves the user to decrypt it using a key shared by the owner and check whether the requested data is the one searched for and send download request to the cloud. The cloud replies with the document which is in encrypted format and the user then decrypts. The MAC is compared with the one sent from the cloud with the encrypted on to ensure it has not been altered.

In [26] , the authors proposed a system called FADE, in short for File Assured Deletion, for data security of cloud that is based on policy (how files can be accessed) and user access control management for assured deletion of data by applying security measures before files are uploaded to the cloud. It is based on an initially devised scheme known as time-based file assured deletion [27] where files are assigned with definite time where they expire and can't be used again i.e. being permanently deleted. For this research there are two bodies that are considered FADE clients (the interface bridges between data sources and cloud that performs encryption and decryption) and Key Managers (stand-alone entities for that maintain policy-based keys, access control and assured deletion). The FADE works effectively both on active user files by fine-grained access control that are stored on the cloud and files have been deleted such that they are not accessible by attackers. This is achieved through using encrypting files using a key (symmetric key) and associating specific policies with them, and further encrypt both files asymmetrically where the asymmetric keys are managed by few third-party key managers that are trusted by clients and the cloud. Introducing FADE required some additional features which introduced new components to the cloud infrastructure, since that is not likely to happen because it requires hardware changes which is difficult to implement, it was designed on thin-cloud interface [28] requiring no new component to be added to the cloud for its support. Thus, the authors used C++ programming language to implement it on top of the existing Amazon S3 infrastructure with two scenarios for file upload and download which brings forth an acceptable

level of computational and monetary overhead. FADE provides privacy and integrity security features.

Wei et al. in [29] proposed a protocol called SecCloud for cloud data storage security and secure auditing of data on the cloud to check whether data on the cloud has been tampered or not. SecCloud achieves security of cloud data using encryption. Three entities are the main focus on SecCloud, they are the CSCs, CSPs and a trusted third party where all three use keys that are created through bilinear pairings which are additive and multiplicative [30]. User's data is chunked into small manageable sizes and are signed by the trusted third-party. After being signed, the CSP and CSC generate session keys to encrypt the signed data using by using Bilinear Deffie-Hellman algorithm [30] and it is sent to the CSP to be stored. Before the data sent by CSC is stored on the cloud it is decrypted first by using the session key, then verification process is undergone on the signature of the trusted third party and once verified to be stored in the cloud. As mentioned earlier SecCloud gives secure auditing feature, this feature is achieved by utilizing Merkle's Hash tree, the results are verified by the trusted third party using probabilistic sampling technique whether the data was tampered or not. SecCloud provides privacy and integrity features.

TimePRE (time based proxy re-encryption) [31] is a scheme developed for data sharing in secure way over the cloud which combines proxy re-encryption (PRE) and hierarchical attribute based encryption (HABE). First the cloud user's data is associated with attributed-based access structure which is declared by the CSC and time limit for access is set which is updated automatically by the CSP after obtaining access request from CSC. Given the above information the data is granted access to users fulfilling both the aforementioned criteria and conditions. In order for the re-encryption to take place a shared key is swapped between the CSP and CSC. Then the CSC encrypts data and sends it to the CSP then the CSP using the pre-shared keys computes the PRE keys and further re-encrypts the initially encrypted data by the CSC and store it on the cloud. It ensures secure communication and user data access revocation based on time constraints i.e. if they expired. The data owner in TimePRE does not have to be online in order to revoke a user from accessing owner's data and to generate new re-encryption keys used for encrypting other files. The access control is ensured by use of ABE that identifies user by set of

attributes rather than identity. The ABE in TimePRE uses eligible time periods for a user along with other attributes to identify a user. This scheme ensures privacy and availability of data.

The authors in [32] introduced a new model of firewall known as tree-rule firewall using tree shaped hierarchical rule sets, which is most suited for large networks such as the cloud. It is a variation for the well-known and used firewall type called listed-rule firewall with time complexity of $O(N)$ where N is number of rules [33] by overcoming its limitations on speed and accuracy of rule set searching by removing redundancy of rules. Rules are arranged in an ascending order in the form of a tree making the search for rules easy and less time and resource consuming with the time complexity of $\text{Log}(N)$, i.e. the firewall starts operation by comparing a packet's header first attribute values with values on the root node and go downwards searching for relevant nodes for the packet values searching through rules and take actions based on the search findings of the firewall i.e. to allow or deny packets to go in and out of the firewall in if-else conditions. The tree rules are constructed at the root in any manner that is desired, such as destination IP, source IP and port address. Tree-rule firewall was implemented on the Linux OS Cent using the Netfilter function and it was tested on two types of hypervisors, Hyper-V (which is windows based and easy to use) and ESXi (frontrunner of virtual machines) alongside with IPTABLES (listed-rule firewall) for comparison purposes. The results of experiments conducted shows that with tree-rule firewall when the number of rules increases per thousand the throughput stays almost constant and does not decline in both cases of the hypervisors while in the case IPTABLES throughput decreases in very high margins.

In [34] the authors come up with a homomorphism distributed verification scheme, which is a kind of a universal hash function initially introduced in [35], to check whether a user's data in the cloud is correct that has been stored redundantly at CSPs i.e. it has not been altered or modified using pseudorandom data that is stored. This feature makes its extensibility limited to small amount of data since it cannot cover all CSCs data stored on cloud but rather small random amounts of data is considered to determine the integrity of data. A homomorphic key is initially computed by the CSC is used to encrypt random user data before being uploaded to the cloud. After storage when the user wants to access his/her data, he/she sends a challenge code to the cloud server where the cloud signs arbitrary data blocks and forward them to the user, where the

user cross checks the received data are the same with the initially encrypted ones using homomorphic keys. Errors are detected that are caused by mischievous cloud servers letting CSC know their data has been tampered with. This scheme ensures data availability, integrity and reliability by securing the cloud against integrity attacks, Byzantine failures and server colluding attacks.

Cloud proof [36] is a method for secured data storage in cloud. In this method users can keep track of their data and make sure it has not been altered and is preserved as it was stored and check to see if there is any misconduct on their data. In articles it is seen that most CSPs Service Level Agreement (SLA) only addresses the availability of users' data 99.9%, when inquired by users like in Amazon S3 [37] and Microsoft's Azure [38]. Thus it attains integrity of CSCs data and additionally provides a security mechanism where proof is provided both for the CSCs and the CSPs to stop false allegations made by each other. Such that a user cannot claim to have been breached his/her data security that was vouched for by the CSP that would not happen and deny when it happens, and where CSCs claim that their data security has been breached and which never took place or made them doubt the CSP. Security in CloudProof is denoted by Integrity, Write-serializability and Freshly-read (IWF) and says security is breached when they do not hold, confidentiality is taken out since the authors considered users can encrypt their data to make it address the issue. Attestation can take place if SLA is violated and parties which claim so can prove the security issues that were not addressed. It was implemented on Window's Azure [39] cloud platform and was found that approximately 15% computation overhead and 10% of throughput declination which is acceptable for the new features introduced and computations conducted. Finally, the authors suggested that SLAs should incorporate the IWF concepts in them in order to become full and where proof can be found for the cloud computing environment.

The researchers in [40] discuss the use of symmetric searchable encryption method using existing cryptographic primitive and order preserving symmetric encryption (OPSE). Though this method failed to deliver security of data stored since it does not provide any information about the security attacks, confidentiality and integrity.

In [41] the authors introduced a cloud adoption framework called Cloud Computing Adoption Framework (CCAF) which is achieved by integrating various security mechanisms (firewall, identity management and intrusion prevention systems, and encryption) at various layers of the cloud. The design for the framework originated from CSCs, CSPs, cloud system providers and other stakeholders. CCAF was implemented and simulated using a Business Process Modeling Notion (BPMN) on various scenarios like data at storage and data at transmission. BPMN is a tool which is used to identify business processes and conduct simulations on them in order to identify which are hugely affected and preserve them from being vulnerable to improve business. Penetration testing was performed on the framework on 10 petabytes of data that was located at University of London Computer Center (ULCC) using the scenarios mentioned above. The experimental set up was composed of 100 virtual machines (VMs) embedded with CCAF (multi-layer security) and another 100 VMs with McAfee Antivirus (single-layer security) by using 10,000 viruses and Trojans which were injected all at once and at 5 hours' interval to check whether how many can penetrate through the multi-layered and single-layered security solutions. Thus based on the experiments 5,423 viruses and Trojans were blocked by the firewall, additionally 3,742 were stopped by the identity management and intrusion prevention systems and 82 were blocked by encryption making it almost all malicious codes could not penetrate through the CCAF with test result of more than 99% when all malwares were injected at once and 76% when injected in 5 hours difference, where in the first case which is 20% greater than single-layered security yielding in more security. Additionally, the researchers found out that it could take up to 50 hours to protect a 2 petabytes data and up to 125 hours to take over control and separate infected files from the uninfected.

In [42], the authors proposed a framework for secured data storage and transmission based on three processes. For the case of this research two parties are taken into account, these are the sender and the receiver. It starts with classification where user distinguishes own data based on confidentiality, integrity and availability where the third one is inversely proportional with the remaining two and the first and second are directly proportional on the basis of the frequency. Then an index builder is utilized to travers through encrypted files making searching functionalities easy on them. The indexed files are encrypted for better security. The third process is encryption, various encryption algorithms were used, initially RSA is used to compute

private and public keys that are used preserve the data confidentiality by authenticating sender and receiver. In order for these key pair to be generated Secure Shell (SSH) was used. Following that a hash function is used and the message to be sent goes through the function and hash of the message is computed. The sender then uses his/her private key and encrypt the hashed message and send it along with the unencrypted original message. Additionally, a symmetric key which is commonly shared by sender and receiver is used again to encrypt the message. Finally, the sender uses the receivers public key and encrypts all the above mentioned encrypted files and sends it to the receiver. The receiver then uses his private key to decrypt the message first and obtains the symmetric shared key where he/she compares it with his/her own shared key where he/she uses it along with the sender's public key to decrypt the message and uncover the original message sent. At last the hash of decrypted message is computed in order to identify whether data has been tampered or not by comparing it with the hashed message sent from the user. This framework was tested and implemented on Hadoop, it also shows that the combined use of the above techniques (HMAC, encryption, classification and indexing) yield's better security.

The authors of [43], devised a generic cloud security framework for cloud, by taking into account three challenges that prevail in cloud computing. These challenges are security and privacy requirements of the cloud, attacks and threats in the cloud, and concerns and risks that are unique to the cloud along with their security solutions. In the security and privacy requirements issues like confidentiality, authentication, authorization, integrity, availability etc..., whereas in the attacks and threats wrapping attacks, browser-based attacks, cloud injection attacks and metadata spoofing attacks etc..., and in the concerns and risks access control, monitoring, application development, encryption, data retention and testing etc... were studied and the possible security solutions were put forth. Thus, based on the studies performed above a security model is formulated which is embedded within the existing cloud environment. It is consisted of four unites namely verification and validation unit, privilege control unit, data protection unit and attacks detection/prevention unit. The verification and validation unit is in charge of authenticating users and ensuring the correctness of their data and services by using One Time Password (OTP) and Two-Factor Authentication (2FA) since cloud is a multi-tenant environment. The second unit is the privilege control unit which takes care of privacy, data integrity and confidentiality issues using rules and policies that determines which stakeholders in

the cloud have the permissions to perform computations on the cloud by using encryption/decryption algorithms like AES. The third security unit is the data protection unit which makes sure that users data stored is protected at all times and also retrieval and removal processes are protected, techniques like truncation, redaction, obfuscation, Hash Functions and MAC can be used to preserve the data security of cloud. The fourth and last protection unit is attack detection/prevention unit which protects the cloud from any anomalies or threats like viruses and intruders that have negative impacts on the smooth operations of cloud services, firewalls, IPS/IDS and connection limiting mechanisms should be used.

In [44] the authors used Auditing Algorithm Shell (AAS) to secure users information on cloud. They introduced a four layered architecture comprising of secure transmission of data, encrypted data and encrypting data processing, database secure shell and internal and external auditing shell for securely streaming data to and from the cloud. Firstly, secure data transmission is performed so as to prevent passive attacks where CSCs data is encrypted and additional fake data is incorporated to the originally encrypted data which is again encrypted in order to confuse attackers and assure secured streaming communication. The fake data ratio with the encrypted one is determined by the users which is transmitted through the network in the same form. Then the encrypted data is processed by the cloud as is and obtained by client, who performs various operations on it in order to obtain the original message to prevent data breach attacks at the cloud. Thirdly, secure shell a database layer that preserves data security of CSCs while it is stored in the cloud. It generates logs of data access attempts along with which server tried to access the data by collecting time stamps, network address stamp and location stamps while responding to access requests from servers, which are used for auditing purposes. Finally, internal and external auditing layer is found which is a means for building trust of CSCs. In this layer the auditing can be performed both internally or externally but no data unencrypted is conveyed to the auditors i.e. only the access logs are presented at the time of audit and it is used to identify any misbehaving/malicious activities on the basis of access time, access location, access network etc... The addition of these four layers introduces computational overhead which is also another issue to consider while implementing this framework. Generally, this framework achieves passive attack detections, access log generation, trusted third party access and, internal and external auditing in a secure manner.

[45] devised a control framework for secure cloud computing, where they introduced a governing body framework that is responsible for creating trust between CSPs by giving attack information that has occurred on other CSPs, it also acts as an interface between CSPs and CSCs, which is a mediating party. This governing body provides these functionalities data center control (from the basic layout of the data centers to how they operate), policy creation and control (from drafting a security policy to implementation and control), increase user awareness (from specifying procedures and methods followed by users to making users aware), legal control (from acquiring global laws related to the cloud to taking care of legal matters of cloud operations), performance evaluation (from assessing performance of CSP to giving ranks based on their performance) and handle conflict and dispute resolution (from computing security parameters that have conflicts to resolving disputes and revoking CSPs licenses) to solve challenges arising from the above mentioned issues. Additionally, the governing body can take measures when CSPs are not abiding by the rules it made, provide security solutions that enhances cloud security, follow up on activities of CSPs to make the cloud more conducive to CSCs.

In [46] the authors proposed a security framework for personal cloud computing. Initially, users (who utilize different devices are authenticated through multi-factor authentication by end-user service portal) are certified by a third party certificate authority in order for them to gain access to cloud services. Then they go through a security control layer know as end-user service portal, where various security activities are performed such as authentication and authorization, this layer is the gateway to let requests in to the cloud and to give service out to CSCs. The end-user service portal provides security control (provides security control for access control, security policy, key management against security threats), service configuration (where service interoperability and integration based up on user's requests is performed using a markup language called SPML (service provisioning markup language)), VPN management (manages the services that are provisioned with the type of VPN connections for each service), service broker (where cloud resources are mapped with user requests) and service gateway (manages network resources), service monitoring (which guarantees high level of service performance and availability) functionalities. This whole process can be used for seamless integration between different CSPs when cloud orchestration is realized.

In the research [47], the author developed a data security framework for the payment card system in Ethiopia. In order to formulate the framework, the author conducted a series of interviews with subject matter experts and reviewed various related researches conducted on payment card systems. He used various tools in order to achieve secure cloud communication of payment industry such as CrypTool2 for encryption and decryption purposes by incorporating different encryption algorithms such as AES, RSA and hash algorithms, and CloudSim for simulating the cloud data center environment which is implemented using the Java programming language. The framework was embedded on the existing banking applications and additionally gives access control mechanisms. But, the simulation was not shown clearly and the findings were not put forth.

2.5. Summary of Related Works

The above stated related works are summarized in the table below by clearly speculating the objective of the researches, the methodologies used, the findings they brought forth and future endeavors to be undertaken.

Table 2.2: Summary of related works

Author	Objective/ Purpose	Approaches/ Methodology	Key Findings	Weaknesses, Extensions & Improvements
S. K. Sood [25]	<ul style="list-style-type: none"> Use combined approaches MAC, data classification and indexing, and encryption to provide complete security of cloud computing ranging from transmission up to storage. 	<ul style="list-style-type: none"> Experimental 	<ul style="list-style-type: none"> The combinational use of MAC, data classification and indexing, and encryption yields higher level of security than using individually the above stated mechanisms 	<ul style="list-style-type: none"> The security measures i.e. MAC (since it is a symmetric key operation) and the data classification process brings forth low level of security to the overall framework
O. Mushtaq et al. [44]	<ul style="list-style-type: none"> Develop a maximum security and privacy attaining system for the cloud (four-layer system) Develop auditing mechanism that is defined by users 	<ul style="list-style-type: none"> Experimental 	<ul style="list-style-type: none"> The four layered architecture provides data security, data privacy and protects against breaches Introduced internal audit, additional to the external audit mechanism for cloud 	<ul style="list-style-type: none"> The authors claimed their framework protects CSCs data from passive attacks but they have not shown how it is achieved
H. Srivastava et al. [45]	<ul style="list-style-type: none"> Introduce a governance body which acts as a mediatory between CSPs and CSCs for its security Improve trust level between various CSPs 	<ul style="list-style-type: none"> Survey 	<ul style="list-style-type: none"> Fills the gaps seen where CSPs are failing to deliver some security objectives 	<ul style="list-style-type: none"> The architecture lacks in describing where to put technical security solutions (like encryption), performance measurement techniques and resource management issues, it only emphasizes legal control (thus incorporating more other cloud adoption issues would have been better) to make it comprehensive
S. Na et al. [46]	<ul style="list-style-type: none"> Propose a cloud security service model and security framework Achieve secured seamless CSPs integration 	<ul style="list-style-type: none"> Survey 	<ul style="list-style-type: none"> For the security framework design identification of security requirements, attack types, threat types were mandatory 	<ul style="list-style-type: none"> Modifying of the framework so that it can be used in cloud orchestration (for seamless integration between CSPs)

Y. Tang et al. [26]	<ul style="list-style-type: none"> ▪ Propose a cloud data security storage system known as FADE based on policy, access control management, attribute based encryption and assured deletion 	<ul style="list-style-type: none"> ▪ Experimental 	<ul style="list-style-type: none"> ▪ Computational overhead incurred due to the introduction of the security system but performance and monetary values were not affected 	<ul style="list-style-type: none"> ▪ The cryptographic key managers are trusted ones but how they are selected to be given such privileges is not stated, so that some security breaches can prevail through it
L. Wei et al. [29]	<ul style="list-style-type: none"> ▪ Devise a protocol for cloud data security and auditing known as SecCloud 	<ul style="list-style-type: none"> ▪ Experimental 	<ul style="list-style-type: none"> ▪ The protocol provides privacy and integrity features but with computational overhead of acceptable amount 	<ul style="list-style-type: none"> ▪ Improve the efficiency of the SecCloud since it introduces latency and increases response time in the cloud and implement it on real cloud platform environments like Amazon S3 or Microsoft Azure for its applicability
Q. Liu et al. [31]	<ul style="list-style-type: none"> ▪ Secure data sharing scheme for cloud called TimePRE where user access to resources automatically expires after a specified period of time 	<ul style="list-style-type: none"> ▪ Experimental 	<ul style="list-style-type: none"> ▪ Efficient when the access time of each users is predetermined 	<ul style="list-style-type: none"> ▪ TimePRE should allow users with different attributes (that is based on access structures) to have uniform time of execution/performance.
X. He et al. [32]	<ul style="list-style-type: none"> ▪ Introduce a tree-rule based firewall 	<ul style="list-style-type: none"> ▪ Experimental 	<ul style="list-style-type: none"> ▪ As the number of firewall rules increased the throughput stays constant which is an advantage over other firewall types 	<ul style="list-style-type: none"> ▪ Make tree-rule firewall applicable to NAT (Network Address Translation), IPv6 and VPN (Virtual Private Network), and make it communicate directly with the hypervisor
C. Wang et al. [34]	<ul style="list-style-type: none"> ▪ Propose an effective and flexible data integrity preservation scheme using homomorphic token and distributed verification mechanism 	<ul style="list-style-type: none"> ▪ Experimental 	<ul style="list-style-type: none"> ▪ Achieved storage correctness verification and identification of misbehaving servers to track the range of errors and take corrective measures ▪ The scheme is highly efficient and resilient to Byzantine failure 	<ul style="list-style-type: none"> ▪ Enforce public verifiability using this model ▪ Solve problems encountered with fine-grained error localization in the scheme as an improvement

R. Popa et al. [36]	<ul style="list-style-type: none"> Introduce CloudProof (for proof for integrity, write-serializability and read freshness) which is practical for data storage in the cloud. 	<ul style="list-style-type: none"> Experimental 	<ul style="list-style-type: none"> High degree of latency is present when using CloudProof but with high scalability 	<ul style="list-style-type: none"> The physical security of the datacenters is not considered in CloudProof as a security risk for cloud
V. Chang and M. Ramachandran [41]	<ul style="list-style-type: none"> Introduce a cloud computing adoption framework (CCAF) a multi-layered security framework (using access control and firewalls, IPS/IDS and encryption) by incorporating technical design and implementations, governance and policies 	<ul style="list-style-type: none"> Experimental 	<ul style="list-style-type: none"> The framework yielded 99% security giving more security benefits (which is multi-layered) than using commercial cloud security solutions 	<ul style="list-style-type: none"> Improve data security and recovery processes in CCAF as the users files increases (performance of CCAF is subject to size of users data)
A. Bhandari et al. [42]	<ul style="list-style-type: none"> Framework for secure data transmission and storage over cloud 	<ul style="list-style-type: none"> Experimental 	<ul style="list-style-type: none"> Combined (RSA and hash functions) use of security mechanisms yields better security 	<ul style="list-style-type: none"> Prove the algorithm mathematically and determine the time complexity on a well-established CSP
A. Youssef and M. Alageel [43]	<ul style="list-style-type: none"> Proposed a generic cloud computing framework 	<ul style="list-style-type: none"> Survey 	<ul style="list-style-type: none"> The framework achieves privacy and security requirements of the cloud 	<ul style="list-style-type: none"> More researches should be conducted on management of risks in the cloud using qualitative and quantitative risk analysis methods to better enhance the framework
E. Endalew [47]	<ul style="list-style-type: none"> Design cloud data security framework for payment card system in Ethiopia 	<ul style="list-style-type: none"> Experimental 	<ul style="list-style-type: none"> Integration of encryption algorithms and access control methods gives more security 	<ul style="list-style-type: none"> Measure the performance of the framework and enhance the data transfer process

Though the frameworks mentioned in the table above contribute to the security of cloud computing, they lack some key features that should have been considered when developing the frameworks. The articles [25,26 and 29] mostly focus on encryption as a mechanism to secure data storage in the cloud, where other cloud security mechanisms are not given much attention and considered in the development of their frameworks. In [44] cloud security is seen from storage perspective by providing internal and external auditing and also from secure transmission of data using encryption mechanisms but does not address other security concerns of the cloud.

[36, 43 and 47] does not take into account the physical security of the datacenters which is one of the most common source of security risk in the cloud, that CSPs should comply with or assure in order for them to be adopted.

In [32, 41 and 42] the adoptability of the frameworks is in question due to quality of service (QoS) degradation the frameworks bring to the cloud. They introduced additional computational overhead that is not tolerated in the scenario of cloud computing where the speed by which services are rendered on-demand and quickly.

As depicted in [48] cloud computing security is not just a technical problem, it also involves other issues like standardization, supervising mode, laws and regulations, and many other aspects. This brings forth for the necessity of an integrated framework which addresses the broad spectrum of cloud computing security using IT governance, which is the main goal of this research.

Thus, based on literatures its evident that the data security mechanisms used for cloud computing are mostly built on technical solutions as seen above which are not enough to make the cloud more secured and adoptable by CSCs. The physical security, the SLAs, policies, governance structures and standards which help by combining them with technical mechanisms for cloud security should be worked on and dealt with. And hence, in this research work the researcher proposed an IT governance framework for improved cloud security by addressing the aforementioned security issues and challenges.

Chapter Three

Research Design and Methodology

3.1. Overview

A research design and methodology chapter covers a lot of ground by depicting each and every step undertaken for designing and conducting the research [67]. In this chapter, the research design, the research samples and methods used for data collection, ethical considerations of the research and the overall course of action to devise the proposed IT governance framework for cloud computing are discussed. Various methodologies are depicted below such as data sources, sampling techniques, data gathering instruments, procedures, analysis techniques, validation and evaluation, IT governance tools and frameworks.

3.2. Research Design

Research design shows the procedural plan or course of actions taken in order to identify and collect data to provide the reader with how the approaches utilized were scientific and systematic [67]. In order to achieve the research objectives and achieve the desired outcome the following measures were taken, first the researcher issued support letter from SMU which was used for contacting and inquiring organizations, then interview guide was developed, following that the interview was conducted at the selected organizations where door-to-door inquiry was made to identify the organizations which use cloud services to run their day-to-day activities and meet their computing needs. After that, based on the interview guide mentioned above a face-to-face interview was conducted. Then, the collected data was analyzed and conclusions were drawn from it, which was used as an input for the security framework formulation. Finally, the security framework developed was validated for its effectiveness and usefulness in solving the problems faced by CSCs and CSPs.

3.3. Sources of Data

To get valid and reliable data, the use of appropriate data sources is very important. Therefore, the sources of data for this study included both primary and secondary sources. The primary data is collected from the IT experts working in the selected organizations who has years of working experience. The secondary source of data gathered from IT security policies, procedures and manuals from the organizations under the study, books, journal articles, conference proceedings and websites.

3.4. Sample Design

In this subtopic the issues discussed below are the target population for the research, the sampling techniques and sample size.

3.4.1. Target Population

A target population refers to the entire group of people, events, or things of interest that the researcher wishes to investigate [44]. The target population and respondents selected for this research were organizations in Ethiopia operating in different sectors like governmental organizations, financial organizations and NGOs, which use cloud computing services and CSPs. The major criteria used to select the organization were active involvement and use cloud computing services. This strategy helped the researcher to collect a more representative view of a population of interest, thus supporting the ability to apply findings to the cloud computing user population at large. Ten organizations from the above mentioned sectors were contacted and only the five were using cloud services and these were selected for study in this research.

3.4.2. Sampling Technique

In conducting the research purposive sampling technique was utilized; more specifically, expert sampling since the IT governance framework for cloud security devised is centered on organizations which uses cloud services and have IT security professionals with known or demonstrated experience and expertise in the area. The reason behind choosing this approach is, it's the best way to elicit the views of professionals who have the expertise deeply.

3.4.3. Sampling Size

Due to the limitation of companies which migrated to the utilization of cloud services and resources a total of 10 IT professionals and IT security professionals based on their availability from 5 organizations that have of experience in managing cloud computing services for their organizations were selected for an onsite interview on this study.

3.5. Instruments of Data Collection

For the purpose of data collection in this research interview and document analysis were conducted. Since the framework developed needs deep analysis of the study population about the cloud services utilized and how they protect them from malicious anomalies the researcher moved forward with such intents. The interview was of great help in order to extract the necessary information from the IT experts for the formulation of the security framework. The process undertaken for data collection are discussed below.

3.5.1. Interview

For the purposes of data collection an interview guide constituting of 11 questions was developed by the researcher and the advisor, which was used to extract the necessary information for the development of the cloud IT governance framework from the interviewees.

In collecting the necessary data, a face-to-face interview was conducted by the researcher using the semi-structured interview questions mentioned above. A semi-structured interview is a qualitative method of inquiry that combines a set of open-ended (questions that prompt discussion) and close ended questions with the opportunity for the interviewer to explore particular themes or responses further. The responses of the respondents were recorded using the researcher's smartphone and by taking detailed short notes. These interviews were very important to gain information about the existing cloud computing services and problems that emerge due to lack of governance of these services. The interview guide is found below at the appendix part of the document (See Appendix C).

3.5.2. Document Review

Document review is a way of collecting data by reviewing existing documents as secondary source of data. Documents may be books, journal articles, conference proceedings and websites were reviewed [67]. Some of the documents include IT security policies that are developed by the studied organizations, IT procedures and manuals and work flow documents found at the studied organizations.

3.6. Procedures for data collection

The procedures the researcher followed are below mentioned which are set of steps undertaken, before conducting final interview, the crafted interview questions were pre-tested for their soundness, clearness and value for the research. A discussion and pre-test of the drafts was made with the research advisor. Thus, by taking the inputs obtained from the advisor into account, the interview questions were enhanced. That means, questions found to be grammatically incorrect and unclear were improved and cleared out. SMU student support office provided the researcher with a support letter for the selected organizations in order to get full support and cooperation from them in gathering the required data, (See Appendix D). Finally, a semi-structured interview was conducted and relevant responses were obtained from the respective organizations (See Appendix C for the interview guide developed).

3.7. Method of Data Analysis

The gathered data from the on-site interview was analyzed qualitatively. The researcher used qualitative approach since the population under the study are few. Thus in order to obtain detailed and specific themes from them the collected data was analyzed word-by-word. Inductive method was used because it is a comprehensive and suitable method used where little or nothing is known about the study [67] where in this research area, no work has been done on the use of IT governance for the purposes of cloud security. The analysis was conducted in a such a way that the themes for the research such as the organizations strengths, weaknesses, gaps and opportunities would be clearly identified and carefully considered when developing the cloud security IT governance framework.

3.8. Validation

The validation of the final proposed security framework was made through showcasing the developed cloud security framework to the individuals i.e. IT security professionals who took part in the interview phase of the research. Additionally, validation of IT security professionals from other organizations on the framework was also taken into consideration. This was how the proposed framework was validated. In addition to the fore mentioned validation technique the researcher made comparison of the various frameworks under the review of related works section of the research with the proposed framework.

3.9. Ethical considerations

The data collection process was performed initially by issuing a support letter from SMU's student support office to the respective organizations under the study. Before conducting any of the interviews the researcher gave the interviewees a consent form to be signed by them specifying that they are willing and comfortable to take part in this research which they agreed to and signed. Additionally, an information sheet was given to them stating the nature of the research, the average time to complete the interview, the confidentiality of the information gathered and the overall idea for conducting the research, which helped in informing the interviewees to understand the motive behind conducting this research (See Appendix A - B).

Chapter Four

Data Presentation and Analysis

4.1. Overview

In this chapter the collected data from the interviews were analyzed and interpreted in a way they give sense and direction to the proposed cloud security IT governance framework. This section is comprised of data analysis and interpretation, and data presentation subsections which are discussed below.

4.2. Data Analysis and Presentation

The organizations under this research were selected based on their usage of cloud computing. Since in Ethiopia there are very few organizations using cloud services they were selected by the researchers purposively as mentioned in the previous chapter.

The five organizations selected for this research were from governmental organizations Information Network Security Agency (INSA) and Ministry of Innovation and Technology (MinT). Next comes the financial organizations that use cloud services which are Debu Global Bank S.C and Enat Bank S.C, lastly from the NGO sectors operating in Ethiopia Save the children were the organizations under study. The detailed description of the analysis process is discussed in the next subtopics.

4.2.1. Information Network Security Agency (INSA)

The first organization where the interview was conducted was at INSA, which is a national cyber security organization established in 1998 E.C. The agency is established in order to defend the country's key infrastructures from cyber-attacks and achieve national interest where currently there are more than 2000 employees working at the agency.

The department that was under this research was Secure Systems and Data Center department that is found at the cyber security division, which is one of the main departments that highly

engages in research and development of cloud services and systems. There are 20 staff members in this department working on the fore mentioned technology areas. Nationally and for the agency's internal use there are projects that has been implemented on the areas of cloud computing solutions which were developed at this department.

Currently, at the agency there is no IT governance framework that is implemented and functional for managing its IT infrastructures. There is a national standard developed at the agency known as Critical Mass Cyber Security Requirements Standard (CMCSS) which enforces the government organizations to put security baselines in order for them to defend their infrastructures from cyber-attacks.

Since the agency is running various systems in order to meet its objectives, one of the services is cloud computing. There is an IaaS that is highly used for internal uses which is deployed over open stack which is an open source cloud deployment platform. For securing the infrastructures of this IaaS there are different technical security controls (centralized security controls) put in place such as IDS, firewall (firewall as a service) and encryption (SSL) to mention some. Additionally, some international standards and best practices for security like NIST's technical security procedures were used to make the IaaS secured. The agency provides cloud computing services to governmental organizations and other departments within the agency which need computational services.

But there were no governance and management means at the agency while providing these cloud services. Such as no SLA, policies and procedures with roles and responsibilities and compliance with industry specific and international data handling, processing and storing.

Based on the interview conducted by the researcher there was no formal way to manage the cloud services like an IT governance framework at the agency. Thus, there are various challenges that arise because of the absence of such framework that incorporates technical and non-technical security mechanisms that guides the usage, implementation and protection of their cloud service.

4.2.2. Ministry of Innovation and Technology (MiNT)

The Ministry of Innovation and Technology (MiNT) is another governmental organization under this research which uses and gives cloud web hosting and storage services to other governmental ministry organizations. MiNT is formed by combining two governmental organizations formerly known as the Ministry of Innovation and the Ministry of Information Communication Technology (MCIT). MCIT which highly engages empowering the nations governmental organizations and people with technology and updating them on new and trendy technological advancements for the purposes of the country's developments. Ministry of Innovation was also highly engaging in innovators in the country with the potential in science and technology by funding scholarships and giving financial aids.

The ministry organization has been structured as follows, at the top there is the MiNT minister, below are the two deputy ministers for the Innovation Development and, ICT Development and Management.

MiNT currently provides various services such as issuing of ICT company certificate for professional competency, provision of telecommunication resale services, telecom value added services licensing, web hosting, domain name registration, etc... In addition, to the aforementioned services given by the ministry develops and enforces nationally rules and regulations such as the national ICT policy and ICT laws.

MiNT implemented a private cloud computing service which is open for use by the other national ministry organizations. These services are used at MiNT and also given to other governmental ministry organizations in the form of IaaS for storage and webhosting purposes and SaaS government organizations web portal respectively. In the use and provision of these cloud services various security mechanisms are in place such as the national firewall, IDS/IPS systems, SSL (encryption), physical security for the cloud servers and international best practices for cloud security.

As a CSP the ministry does not provide any SLA with the respective users on the service delivery mechanisms and other means of transparency and auditing mechanisms are not provided.

Though, all these technical security controls are in place they don't cover the end-to-end security aspects of cloud computing risks, vulnerabilities and threats as seen in the previous chapters. Additionally, the availability of non-technical security mechanisms stated above with the roles and responsibilities with formal work flows should be in place to minimize the risks and provide CSCs confidence on the services they get.

4.2.3. Dehub Global Bank S.C

One of the financial organization where this research focused on is Dehub Global Bank S.C, which joined the banking industry in 2004 E.C. with a capital of 266.9 million birr. This bank is a new comer relative to the other bank in this research and currently with 400 employees onboard.

There are different directorates that operate within the bank in order for it to achieve its missions and objectives. One of them is the IT directorate which is organized into three departments working under it, these departments are the System, Infrastructure and E-banking departments. The system department have got under it operating three unites namely the Application unit, Database unit and Development unit working on the software and systems the bank utilizes for conducting day-to-day banking operations. The infrastructure department whereas consists of the IT security and, Network and Support units that works on the securing and development of the various infrastructures and systems owned by the bank. In the IT directorate a total of 15-20 employees are found from seniors with working experience of more than 6 years of professional IT to junior ones with 2 years of experience.

There are IT policy and procedure documents that are developed for the IT infrastructures and services that encompasses the user acceptance policy, system policy, infrastructure/equipment policy, data center policy etc... used for controlling and managing the IT systems and infrastructures of the bank.

Dehub Global Bank uses two cloud services SWIFT for conducting money transfer internationally and corporate email since the bank do not own an in-house mail server and SWIFT infrastructures that operated and managed internally. For securing the fore mentioned cloud services 2-Factor authentication, firewall, swift security requirements are deployed.

The security professionals interviewed mentioned that there are security gaps and service discrepancies and they don't have any mechanisms of monitoring them. Additionally, for the two cloud services the bank uses there is no mechanism for them to get performance measurement and the CSP did not provide them with tools to do so too. Information of how the DC of the mail server is monitored and secured is out of their scope and they do not have any SLA signed by the CSP and CSC as a formal legal document used to penalize service interruptions and inconsistencies originating from the CSP. Third party audit features for CSCs to conduct or assess by certified IT auditors are not provided by the CSP thus they regard the cloud service they use is not transparent. The CSPs also did not provide the CSCs with compliance of international laws and standards they abide by, they only provide on the technical security mechanisms they use.

Since there is awareness gap at the top management of the bank in the issues IT security is concerned mainly on the technology part and since there is no record of cyber-attack on the bank, little attention has been given to it to secure the banks services. The IT professionals at the bank also implied for the need to improve the service quality there must be some governance features that must be used to monitor and deal with the service delivery gaps they encounter.

4.2.4. Enat Bank S.C

One of the financial institutions under this research is Enat bank S.C which is a private owned bank established in 2005 E.C. with a startup capital of 263 million birr. Currently there are around 500 employees nationwide at the bank. There are 18 IT staff members working on the various IT departments of the bank.

There is an IT director who is the head of all the departments, where there are five IT departments namely Infrastructure (works on Network and Hardware), System (works on the various banking systems the bank uses), Security (works on securing the systems), Development (works on developing software that are used for internal purposes) and E-banking (works on providing customers with electronic channels mode of transactions). In order to secure the bank's IT infrastructures and systems there are an IT security policy and IT policy addressing various issues such as password policy, physical security policy, asset management, access control,

incident management, etc... Though, these policies are in place their applicability is low since there exists various challenges to manage and secure the IT infrastructures of the bank such as security awareness of employees, lack of the use of genuine software products, budget availability, business operation and security (when enforcing more security controls the business operations are affected and vice versa) imbalances are to mention some.

The bank uses three cloud services one for email, another for performing SWIFT transactions (global money transfer) and website hosting purposes that are hosted in public cloud. Different security controls are used to secure the various cloud services such as encryption, firewall/IPS, IDS and SLA.

All the cloud services are hosted at a public cloud service provider but the SLA signed with the CSP focuses more on service delivery and little or no security issues has been addressed. Other issues like compliance, transparency and governance issues also were not also covered. Thus, the bank has no means of control over the cloud services utilized. This makes the bank vulnerable to the various security threats and attacks mentioned in the previous chapters of the research.

4.2.5. Save the Children

Save the children is an international NGO that was founded 100 years ago which works mainly on children wellbeing, education and health. The organization has been operating in our country for more than 83 years. At this NGO there are around 25,000 employees worldwide and more than 2,200 in Ethiopia working on the various areas of operations mentioned above. From the total employees working internationally at the organization 250 are IT professionals. The Addis Ababa office is where it is the head quarter for Ethiopia is located. There are 8 IT staff members at the Addis Ababa office composed of at the top an IT manager who manages the three sections under him namely Network section, System section and Support section.

There is an IT policy that is enforced at the organization which is cascaded from the international IT policy that is updated regularly (on every quarter annually if applicable). The policy focuses on security, system usage and antivirus and derives from international security best practices. There is a strict enforcement of this IT policy using active directory control mechanisms.

Generally, the security process is managed by an automated mechanism and less involvement of the IT professionals.

The organization's IaaS and SaaS cloud services are hosted on public clouds for conducting day-to-day businesses like Microsoft cloud storage and office 365 respectively. From the interview the researcher found out that 95% of the organization IT services are obtained from the cloud, thus the IT infrastructures used that are found on-site are very small. There are different security controls that are used for the cloud services the organization utilizes such as firewall, multifactor authentication, etc...

There is a signed SLA with the CSP but it mainly focuses on the service delivery issues but does not incorporate how these services security is managed and related issues are handled too. There is no mechanism of managing cloud security from the organization's end, since it is automated which highly relies on the trust of CSP and if there is any intrusion on the cloud servers where the organization's data resides they do not have any means of knowing such activities has occurred like third party audit reports is not provided for the CSC. Thus, the IT professionals working at the NGO does not think the services they get are in transparent manner. They demand to get such features from the CSP to alleviate governing mechanisms for their data at remote servers.

4.3. Data Interpretation

All the interviewed organizations have incorporated their business processes with IT, thus they have a well-structured organizational structure and formed IT departments and in some cases even IT security departments. This can be taken as a strength as to the organizations are giving much attention to security of their IT infrastructures. The CSCs under this study have highlighted the necessity of transparent and open service delivery from CSPs and a way to govern them.

There is no presence of IT governance frameworks at CSPs for managing business process, IT infrastructures and cloud services, and enhancing the security of the organizations. Though the organizations under the study used some measures of IT governance mechanisms for their internal IT services, they didn't use or enquire the CSPs to provide them with means of governing their data in the cloud. The CSPs focus on using technical solutions for cloud security,

as seen from the literature review and related works sections of the research it is not enough to secure their infrastructures leaving other cloud computing vulnerability issues unaddressed.

Awareness of top management as well as the other staff members including technical staffs on the invaluable essence of IT governance for securing their cloud hindered all the organizations under this research from achieving control over their data in the cloud, performing audits for checking if their original data has been tampered or not, any malicious activities have occurred and getting better quality of services.

None of the interviewed CSC organizations has signed SLAs with their CSPs as a means of controlling them from unauthorized tampering, monitoring their usage of the cloud services and improving their usage and confidence on the services they get.

From the various organizations in this research, it is evident that all tried to defend their assets in the cloud and placed different controls to achieve it, but through the use of these controls it can be seen they have not secured their cloud environment, since cloud computing security cannot be achieved only by technical security solutions. In the above section all of them focused on technical solutions and technological means and gave minor or little concern to the non-technical aspects such as governance, standards and policies that affect the security in the cloud. Also the CSPs do not use organized and managed way of securing their services i.e. all the efforts they exert are in ad-hoc manner not in organized and formal manner, which does not cover end-to-end security concerns.

Additionally, the companies using cloud services did not enquire the CSPs on how they deliver security to the services they render. In which there lies a gap on how they are assured the resources they utilize are tamper free and secured to maintain their confidentiality, integrity and availability to their leased services. Companies wanting to shift their services to the cloud have seen huge challenges due to the prevailing security concerns and issues on cloud computing. Thus, the researcher wants to tackle these challenges, security concerns and make the transparency that is hidden to the CSCs visible in order for them to be assured that the services they utilize are secured and gain confidence on using and adopting them.

Chapter Five

The Proposed Framework

5.1. Overview

In this chapter the cloud security IT governance framework that was formulated based on the findings of review of related works, interview and document analysis is shown. Additionally, discussion of the various components of the framework along with scenarios where the proposed is used on various security incidents of cloud. The framework is designed to answer CSCs security questions and issues, and make them comfortable using these services and transparent for them. Additionally, through the use of this framework CSPs make their services more transparent to CSCs, which builds the trust between them and adds confidence to CSCs.

5.2. The Cloud Security IT Governance framework

The framework was formulated taking into consideration the security vulnerabilities that are found and which are introduced through the use of cloud computing and the security mechanisms and controls that are used to minimize them. It gives a high level view of the cloud security mechanisms used and the processes needed to improve cloud security and adoption for customers. Which can be used as baseline security requirements for CSPs when providing computing services. Thus, since the framework states the minimum requirements of technical and non-technical security controls and IT governance mechanisms, and based on the fact that new and emerging cloud computing security vulnerabilities and threats that may evolve, the framework can be modified to accommodate them.

As an IT governance framework the proposed cloud security framework addresses the various domains of IT governance which were discussed in Chapter 2 of this research and answers the security concerns and issues raised by CSCs.

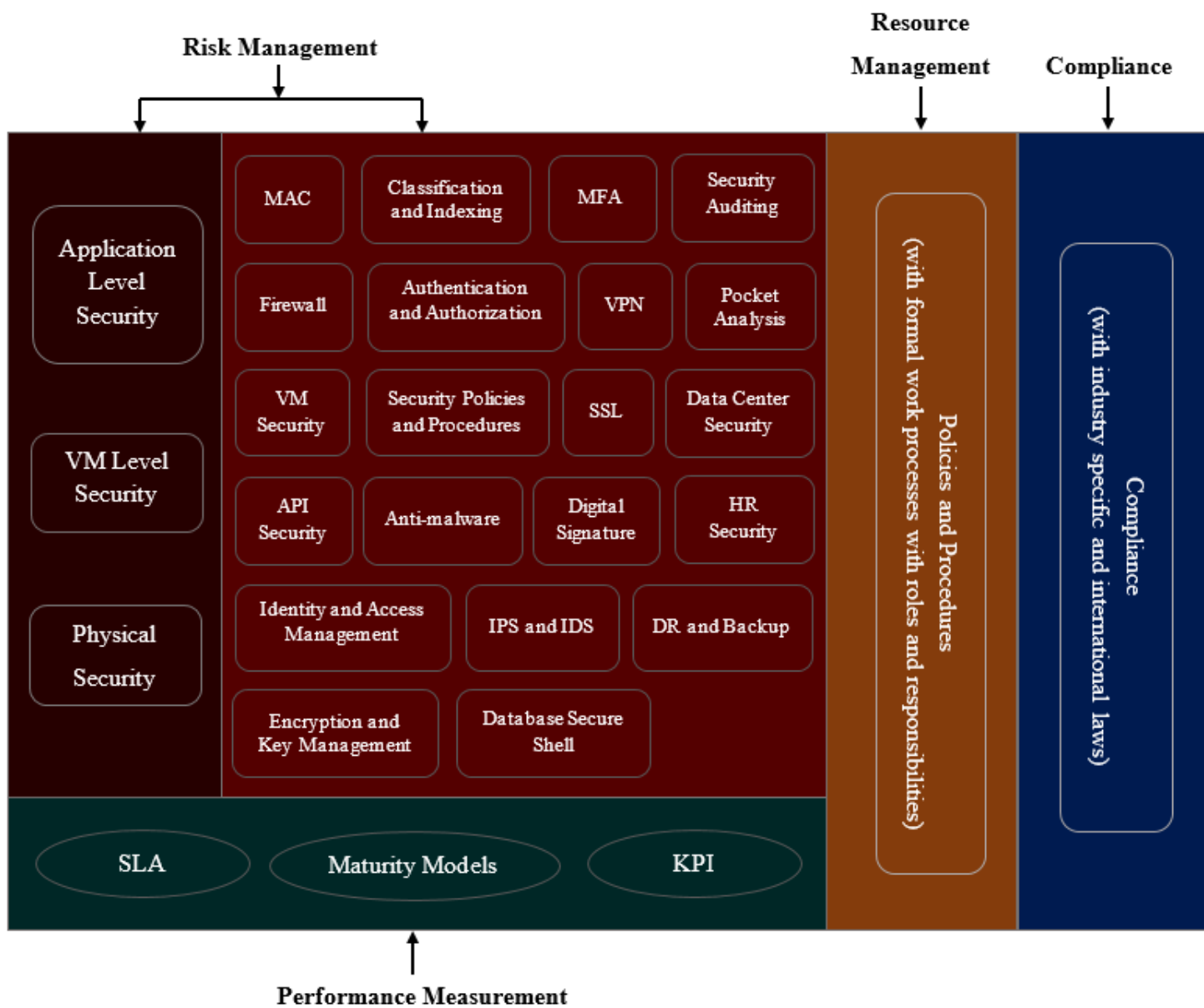


Fig. 5.1: The Proposed Cloud Security IT Governance Framework

The framework depicted in the figure above shows the overall view and components. In the following sections the components are explained in detail and rationale behind the framework is stated.

5.3. Components of the framework

The framework consists of four sections which are discussed in detail below. These sections are composed of the various cloud security solutions (comprising of technical and non-technical security mechanisms) and IT governance solutions in respect to IT governance domain areas, specifically Risk Management, Performance Measurement, Resource Management and Compliance.

5.3.1. Risk Management Section

The risk management section encompasses all the security measures, both technical and non-technical. Initially, the building blocks of cloud computing environment where security concerns arise are categorized as into three parts as Application level, VM level and Physical level. There are different security controls used by CSPs to protect cloud assets at the above mentioned levels.

Here the researcher collectively organized the security controls that are commonly utilized and found at each level which mostly are technical cloud security mechanisms. To mention some, Encryption (where CSCs data should be in encrypted format at storage, at use and during transmission, key management should be handled by trusted third party organ rather than CSPs), Identity and access management (where CSPs use different role based identity and access control mechanisms for managing and securing their cloud assets), firewall and IPS/IDS (where incoming and outgoing traffic and data are filtered and any malicious network activity is detected and prevented from causing damages), datacenter security (where HVAC are used to maintain optimal computational capacity, datacenters are monitored and protected using physical and technological means, DR sites are setup for business continuity), API security (where the API used are tested and secured before being utilized), security auditing (where the CSPs conduct audits at premise and also provide CSCs with audit logs for third party auditing), classification and indexing (where CSPs provide for CSCs with mechanisms to classify their data and based on their confidentiality levels provide them with security controls pertaining to their level), digital signatures (where CSPs servers identify the requests inbound are from their authentic customers and render service based on their digital signatures), MAC (by which customers can check the

integrity of their data at the cloud has not been tampered), VM security (by which the VMs authenticity is checked regularly and any malicious VM is detected and removed and VM encryption). HR security (where CSPs make background checks on the employees they employ for any misconducts or criminal records on their pervious careers). These security mechanisms are majorly used and are not limited to the ones mentioned here, CSPs can utilize other security controls too.

Additionally, CSPs should notify their customers these lists of security mechanisms in order to make them aware of the security depths utilized on the services they provide and boost their customer's confidence and become transparent with these issues. This was one of the issues that was seen from the interviews conducted where CSCs were demanding to know what security measures their service providers are using explicitly.

5.3.2. Performance Measurement Section

The performance measurement section under discussion comprised of the IT governance components that must be incorporated with the technical cloud security mechanisms to deliver transparent services with the capacity of generating reports and delivering on-demand and regular status reports to the CSCs and attract new companies that want to switch to adopting cloud. CSPs should use SLA agreements (where they can specify the quality of service they provide along with the penalty cost they incur when they do not meet the specified service quality), KPI (where CSPs should provide their customers with how they have competitive advantages than other CSPs with their organizational structures and clear designation of roles and responsibilities for these structures to better deliver services in secure and transparent manner). Maturity levels (where CSPs work flows and organizational capabilities are specified in terms of maturity levels from ad-hoc to optimized to make customers aware of the how their services are managed and handled at the service provider).

CSCs also demanded that CSPs should generate reports of service usage, incidents occurred and performance measures in regular and timely manner since performance measurement answers the efficiency of services delivered and future projections on expansion both for CSPs and CSCs.

Thus, CSPs can use additional performance measurement tools to provide better service to their customers.

5.3.3. Resource Management Section

The resource management section of the framework encompasses the cross-dimensional functions which are policies and procedures that are implemented by the CSPs to ensure formal work flows and series of steps undertaken while performing activities related to the work of the CSPs along with their roles and responsibilities.

They cover the API security (where various policies and procedures related to API are utilized at development, deployment, management and maintenance), incident management policy (when incidents occur the formal process of identifying the incident, analyzing it and providing solutions), HR policy (duties and responsibilities of every employee along with penalty measures in the time of misconduct, security awareness trainings should be provided to employees and IT users of CSCs by the CSP), BYOD policy (at CSPs premises to control illegal devices from being used and accessing prohibited servers), identity and access management policy, Datacenter access policies, auditing policy (where CSPs perform internal audits and third party audits of various systems at regular basis and make the reports available to CSCs), data retention policies (for how long should data of customers which are not currently under contract with the CSP), risk assessment policy (for performing regular risk assessment activities to identify new and emerging risks and threats for protecting customers data), identity and access policy (access to cloud infrastructure should be based on clearance level both at CSP and CSC), VM configuration policy (isolation between customers), vulnerability management policy (how vulnerabilities are identified, managed and patches are applied), change management policy (where any changes are made at the CSP environment these changes must be communicated to the CSCs and the customers services are not affected), supply chain management policy (how CSPs handle third party suppliers and vendors of various technology equipment and devices that are used to build their infrastructures and services).

Resource management is one of the domain areas of ITG, thus this framework addresses the issues related with it by establishing formal work flows, processes and organizational structures as seen above that are used at CSPs to monitor and manage resources owned by them.

5.3.4. Compliance Section

Compliance is also another cross-dimensional topic that boosts the confidence of CSCs, which CSPs are adhering to and abide by. The compliance with local laws, international standards, legal issues and industry specific rules and regulations are some of the basic topics CSPs take into consideration while operating and giving service. Additionally, customers should be aware of these compliance to be assured that their data is not stored in a country with no strict security rules and regulations in place.

There are many standards composed of security best practices that CSPs should be compliant based on the services they provide and customers' data they process and store. Industry specific such as HIPAA (Health Insurance Portability and Accountability Act which is used for handling health related data), PCI DSS (Payment Card Industry Data Security Standard for companies processing payment card information), GLBA (Gramm-Leach-Bliley Act for financial institutions protecting customers' information). Additionally, CSPs can be certified in generic baseline standards such as ISO 27001, COBIT and ITIL.

These standards that are applied at different areas such as API compliance (at design, development, test and deployment of system interfaces), VM compliance (VM configuration, deployment and security) and physical security compliance (how datacenters are built, CCTV cameras placement, biometric security measurements to enter premises).

As seen, the proposed framework is composed of different sections that yields better security of cloud computing through the use of combination methods of technical and non-technical security mechanisms. In addition to security, the framework addresses trust issues, interoperability issues, transparency issues which are the major obstacles that are limiting the usage and adoption of cloud.

Chapter Six

Evaluation of the Framework

6.1. Overview

The framework presented in the previous chapter was evaluated in two ways. The first way of validation was conducted by going to the interviewed IT professionals and showcasing the framework to them and taking feedbacks to enhance it. This method of validation is known as member checking [70]. Additionally, the researcher showcased the framework to other non-interviewed IT professionals for their feedbacks. The second means of evaluation was done by comparing the security features used in the related works with the proposed framework.

6.2. Evaluation of the proposed framework

6.2.1. Evaluation from feedback

As stated in the previous section the framework validation was conducted both from the initial interviewed IT professionals and other IT professionals who were not involved at the interview phase, a total of 10 subject matter experts (5 from the interviewed and the remaining from other organizations) were involved in the evaluation of the framework. The number of respondents were limited to 10 because few experts were willing to participate on the research.

The experts were showcased the framework and gave ratings on the it by answering the below mentioned questions and their rating was answers in five levels 1 up to 5 where 1 is the lowest while 5 is the maximum rate given.

- ❖ Do you consider the framework addressed security gaps in the cloud that is faced by CSCs?
- ❖ Is the proposed framework clear to understand and implement?
- ❖ Do you consider the framework addresses the CSCs need for transparency and governance on their data in the cloud?

- ❖ Do you think the involvement of third party audits add to the transparency?
- ❖ Does the framework answer questions compliance and legal issues?
- ❖ Does the framework address the issues of insufficient data security?
- ❖ Does the framework provide mechanisms of alleviating risks of losing control over their data?

The above set of questions were asked to the involved study participants in this research and their responses are depicted as follows

- ❖ Do you consider the framework addressed security gaps in the cloud that is faced by CSCs?

For this question eight of the respondents rated the framework a value of 4 and the remaining two rated it 5. The respondents gave positive feedbacks about the framework since issues that were concerning them as users of cloud computing has been answered by the transparency and governance by the performance measurement section and resource management section. Additionally, the compliance section addresses huge doubts of how their data was processed and stored in the cloud by rules, regulations and industry specific standards.

- ❖ Is the proposed framework clear to understand and implement?

All the respondents answered that the framework was clear and they understood it easily, and gave a rating of 4. Since respondents were technical professionals working on the cloud, they had the full picture on where to place the security components of the framework and how they could implement is easily based on their company's organizations structure and behavior both the technical and non-technical security mechanisms.

- ❖ Do you consider the framework empowers CSCs with the transparency and governance over their data in the cloud?

The respondents gave optimistic views about the framework by rating value of 4 and above about the issues of providing transparency and governance functionalities to the CSCs since there are two sections that are dedicated to these issues the performance management section and resource management section. The earlier one gives mechanisms for CSPs getting audit report,

perform audits by auditors of their own choice and knowing the service maturity levels they get. The latter one provides formal workflows along with roles and responsibilities that CSPs should establish and give highlights of how they are governed to their customers.

❖ Do you think the involvement of third party audits improves the issue of transparency?

Half of the respondents gave the issue of third party auditing a value of 4, whereas two gave a rating of 3 and the remaining three gave a rating of 2. The respondents that gave the least rating were concerned with introducing another party to the cloud environment would bring other vulnerabilities to the existing cloud computing environment and were against it. While the ones that gave the highest rating suggested the use of third party audit enhances the transparency of CSPs with appropriate levels of security in place. Such as only giving permissions for the access log files to the auditors and limited access to CSPs servers so that confidential customers data would not be accessible by these third party auditors.

❖ Does the framework answer questions about compliance and legal issues?

All of the respondents gave a value of 5 about the framework addressing compliance and legal issues. This is because there is a dedicated section that deals with compliance. The respondents believed that CSPs should be complaint to various local and international laws since there are different rules at different countries where the CSP servers reside where CSCs data are stored or transferred. In addition to that CSPs should be certified in industry specific standards to attract customer to using their services and become eligible to operate in freely on different countries to process and store CSCs confidential data.

❖ Does the framework address the issues of insufficient data security?

The issue of data security is not just left out for technical security mechanisms since the cloud environment is composed of many components. Thus all the respondents gave a rating value of 5 since the framework takes into consideration the various stakeholders of cloud computing and minimize the risks and vulnerabilities that emanates from them by combination of technical cloud security solutions and IT governance tools and mechanisms. The respondents addressed that the framework shed a light on the security concerns and solutions of cloud computing should be seen from wider viewpoint rather than the conventional ways.

- ❖ Does the framework provide mechanisms of alleviating risks of losing control over their data?

One of the issues that hinders the adoption of cloud was the loss of control over ones owns data since its stored in remote servers outside the boundary of the data owner. Seven of the respondents rated this framework with 5 and the remaining three gave it a rating of 4. Thus its evident that the framework does alleviate risks of data control loss because CSCs have got the mechanisms of checking their data has been modified or tampered by getting auditing and compliance the where the data is processed and stored in a secure way.

Based on the member checking validation technique, it was evident that the framework has got potential in solving the cloud security issues and concerns emanating from transparency, legal, regulatory, compliance, resource management and risk management aspects. As seen from their suggestion such frameworks are good to attract new customers to the arena and making the ones who already are users to continue using it and expand their use based as their demands increase knowing that the risks associated with cloud computing are managed. Almost all of the respondents agreed with the involvement of third party for auditing and identifying security vulnerabilities and threats are valuable for the secure service delivery to customers.

Since the framework depicts baseline requirements, CSPs can add to the security controls both at the levels of technical and IT governance parts that suits their working environments, the preferences of their customers and to address regulatory compliance issues.

6.2.2. Evaluation by comparison

The various cloud security frameworks that has been devised by different scholars are evaluated against the proposed framework in order to give proof that the proposed framework over arches and covers security issues that are not addressed. This is depicted below along and final summary of the evaluation process is presented. The key comparison criteria were whether the frameworks address physical level security, VM level security and application level security on the cloud environment. Then does any of the devised frameworks provide transparency and accountability features through performance measurement matrix, resource management and compliance.

In [25] the researcher proposed a framework using three security features which are MAC, classification and indexing and encryption for secured cloud computing, but VM related security issues, physical security and API level security issues has not been addressed. Thus, based on this it is not evident that this framework fulfills the security needs of cloud from other dimensions.

The authors of [44] used the technical security control mechanisms encryption, database secure shell and auditing as a cloud security framework. The auditing section tried to cover some transparency issues that was not addressed by many of the other frameworks. But other aspects about the performance measurement and compliance were not dealt with.

In [46] the authors authentication and authorization for cloud security, which is not enough for deeming only using these methods alleviates cloud security issues residing at API and VM levels. Additionally, from the perspectives of resource management and performance were not addressed.

[32], [41] and [43] the researchers used firewall for filtering authentic user requests from malicious ones. Whereas the other cloud computing concerns such as internal attacks, VM level security, performance measurement and resource management were not incorporated in the framework.

[34] used hash functions for the security of cloud computing, where the user computes the hash of every data before uploading his/her data to the CSP's server. Then when the CSC wants to access the uploaded data, the hash of the message is computed and compared to the value before it was uploaded to the cloud, if the values are the equal then the data has not been altered or modified while resting at the CSP. This framework does not cover the security issue of passive attacks, since only alteration of the data elements is considered without knowing whether they have been accessed or not without the consent of the data owner. Additionally, the security issues at the physical server, VM level security, and application level were not addressed.

In [43] the authors used authentication, encryption, hash functions, firewall and IPS/IDS to propose a cloud security framework. These security controls are also not sufficient enough to

regard that they make the cloud computing environment transparent and secured where they can monitor the CSPs activities and work flows.

The researcher in [47] make use of encryption and hash functions to deliver secured cloud computing. Which is not enough to deem these security controls achieve a secured cloud environment from end-to-end since the cloud environment involves various components where vulnerabilities are found. Thus, cloud security frameworks should encompass every element involved and in the cloud computing environment.

Thus, based on the frameworks above it is seen that the combinational use of the various security mechanisms in layered way addresses some portions of cloud security issues but the end-to-end security starting from physical security at the DC of the CSPs to program interfaces design, development and security. Additionally, the transparency and compliance concerns and issues were not addressed.

Chapter Seven

Conclusions, Recommendations and Future Works

7.1. Conclusions

The major activities the researcher undertook in these research were gain the current perspective of cloud computing security challenges and what possible solutions are there to make the cloud better security and adoptable. Then by taking into consideration how organizations in our country are utilizing cloud computing and how they address the globally known security concerns/issues interview, observation and document analysis were conducted. The findings were the CSPs deliver security mechanisms which were not transparent and majorly focus on delivering the rented service rather than securing it using various security mechanisms. So this research was conducted to alleviate the aforementioned issues through devising an IT governance framework tailored for cloud computing.

The proposed framework incorporated various cloud security mechanisms and IT governance methodologies into the cloud operation areas. Majorly the hybridization of these two mechanisms for cloud security is one of the findings of this research, by dividing the cloud computing environment into three levels physical, VM and API, then putting in place technical solutions. These security mechanisms are not enough since the cloud operates outside the perimeters of the customers, thus other tools need to be used in order to address the issues incurred from the remote storage of sensitive customers' data. In order to accomplish that IT governance domain areas are incorporated that gives managing and governing capabilities to customers.

7.2. Recommendations

Cloud computing security concerns and issues are the major obstacles that holds potential customers from moving forward and adopting it. Thus, researches revolving around these topics should be conducted that tries to address the overarching security requirements not only from the perspectives of CSPs but also their customers. CSPs can benefit from this framework by delivering secured, transparent and managed (with distinct roles and responsibilities) that attracts users to use the cloud. CSCs also benefit from this since they can perform audits and monitor the services they use.

7.3. Future Works

The researcher has put forth the following list to be incorporated into the framework to enhance and improve its applicability in future endeavors.

- ❖ Implement the framework at CSPs and assess its efficacy in real-time
- ❖ Since the organizations under this research are few due to time constraints, expansion of the study population is also planned to be conducted
- ❖ Enhance the framework to other address other emerging cloud security concerns due to its dynamic nature
- ❖ Include wide range of CSPs for future and
- ❖ Inquire CSCs who use services which implemented the framework about the benefits they gained

References

- [1] H. Hafiddi, Y. Bounagui and A. Mezrioui, "COBIT Evaluation as a Framework for Cloud Computing Governance", *International Journal of Cloud Applications and Computing*, vol. 6, no. 4, pp. 65-82, 2016.
- [2] T. W. Singleton, "IT Audits of Cloud and SaaS", *ISACA Journal*, vol. 3, pp. 5-8, 2010.
- [3] S. O. Kuyoro, F. Ibikunle and A. Oludele, "Cloud Computing Security Issues and Challenges", *International Journal of Computer Networks (IJCN)*, vol. 3, no. 5, pp. 247-255, 2011.
- [4] "State of Cloud Adoption and Security," *forbes.com*, [Online]. Available: <https://www.forbes.com/sites/louiscolombus/2017/04/23/2017-state-of-cloud-adoptionand-security/>. [Accessed 25 May 2017].
- [5] N. Gonzalez, C. Miers, F. Redígolo, M. Simplício, T. Carvalho, M. Näslund and Pourzandi, M., "A quantitative analysis of current security concerns and solutions for cloud computing", *Journal of Cloud Computing: Advances, Systems and Applications*, 2012.
- [6] Gartner, "DataQuest Forecast on Public Cloud Services," 2010.
- [7] F. Liu et al., "NIST Cloud Computing Reference Architecture", NIST, 2019. [Online]. Available: <https://www.nist.gov/publications/nist-cloud-computing-reference-architecture> [Accessed: 15- Feb- 2018].
- [8] P. Mell and Timothy Grance, "The NIST Definition of Cloud Computing," NIST Special Publication, pp. 800-145, 2011.
- [9] S. Force.com, "Platform as a service," [Online]. Available: <http://developer.force.com>. [Accessed 16 February 2018].
- [10] N. S. Portal, "netsuite.com," [Online]. Available: <http://www.netsuite.com>. [Accessed 16 February 2018].
- [11] R. Krutz and R. Vines, *Cloud security*. Indianapolis, IN: Wiley & Sons, 2011.
- [12] F. Shahzad, "State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions," *The 6th International Symposium on Applications of Ad hoc and Sensor Networks (AASNET'14)*, 2014.
- [13] G. Ramachandra, Mohsin Iftikhar and Farrukh Aslam Khan, "A Comprehensive Survey on Security in Cloud Computing," *The 3rd International Workshop on Cyber Security and Digital Investigation (CSDI 2017)*, 2017.
- [14] "A Research Report on Security of Cloud Computing providers study," Ponemon Institute LLC, 2014.
- [15] A. Omari, "It governance evaluation: Adapting and adopting the COBIT framework for public sector organizations," Queensland University of Technology, Australia, 2016.
- [16] P. Stanojevic, "An Assesment of the IT Governance Maturity at SL", MSc Thesis, Royal Institute of Technology (KTH), Sweden, 2011.
- [17] P. Weill and Jeanne Ross, "A Matrixed Approach to Designing IT Governance," 2004.
- [18] C. Leonardo, "IT Governance: A framework Proposal, and an empirical study," Rome, 2008.
- [19] B. Senait, "IT Governance in Ethiopian Financial Sector: A case Analysis of Commercial Bank of Ethiopia (CBE), Korea, 2011.
- [20] T. Asnake, "Tailoring IT Governance Framework for National Bank of Ethiopia," 2016.
- [21] M. Sallé, "IT Service Management and IT Governance: review, comparative analysis and their impact on utility computing", HP Research Labs, Palo Alto, 2004.
- [22] M. Tagel, "Maturity of Information Technology Governance in the Financial Sector of Ethiopia;a 89 Comparative Study," Addis ababa, Ethiopia, 2016.
- [23] ISACA. COBIT 4.1 Excerpts, USA: IT Governance Institute, 2007.
- [24] H. Susanto, M. Almunawar and Y. Tuan, "Information Security Management System Standards: A Comparative Study of the Big Five", *International Journal of Electrical & Computer Sciences (IJECS-IJENS)*, vol. 11, no. 05, pp. 23-29, 2011.
- [25] S. K. Sood, "A combined approach to ensure data security in cloud computing," 2012.

- [26] Y. Tang, P. Lee, J. Lui and R. Perlman, "Secure Overlay Cloud Storage with Access Control and Assured Deletion", *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 6, pp. 903-916, 2012. Available: 10.1109/tdsc.2012.49.
- [27] R. Perlman, "File System Design with Assured Delete," *Proc. Network and Distributed System Security Symp. ISOC (NDSS)*, 2007.
- [28] M. Vrable, S. Savage and G.M. Voelker, "Cumulus: Filesystem Backup to the Cloud," *ACM Trans. Storage*, vol. 5(4), no. 14, 2009.
- [29] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen and A. Vasilakos, "Security and privacy for storage and computation in cloud computing," *Inform. Sci.*, p. 371–386, 2014.
- [30] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *SIAM Journal on Computing*, vol. 32, no. 3, p. 586–615, 2003.
- [31] Q. Liu, G. Wang and J. Wu, "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment," *Inform. Sci.*, p. 355–370, 2014.
- [32] X. He, T. Chomsiri, P. Nanda and Z. Tan, "improving cloud network security using the tree-rule firewall, Future Gener," *Comput. Syst.*, vol. 30, p. 116–126, 2014.
- [33] A. Shebanow, R. Perez and C. Howard, "The Effect of Firewall Testing Types on Cloud Security Policies," *International Journal of Strategic Information Technology and Applications*, vol. 3, no. 3, pp. 60-68, 2012.
- [34] C. Wang, Q. Wang, K. Ren and W. Lou, "Ensuring data storage security in Cloud Computing", 2009 17th International Workshop on Quality of Service, pp. 1-9, 2009. Available: 10.1109/iwqos.2009.5201385.
- [35] L. Carter and M. Wegman, "Universal Hash Functions," *J. Computer and System Sciences*, vol. 18, no. 2, pp. 143-154, 1979.
- [36] R. Popa, J. Lorch, D. Molnar, H. Wang and L. Zhuang, "Enabling security in cloud storage SLAs with cloudproof", Microsoft Research, 2010.
- [37] "Amazon s3 service level agreement," AMAZON, 2009. [Online]. Available: <http://aws.amazon.com/s3-sla>. [Accessed 09 November 2018].
- [38] "Windows Azure Pricing and Service Agreement," MICROSOFT CORPORATION, 2009. [Online]. Available: <https://azure.microsoft.com/en-us/pricing/?v=18.43>. [Accessed 14 November 2018].
- [39] "Windows Azure," MICROSOFT CORPORATION, [Online]. Available: www.microsoft.com/windowsazure. [Accessed 7 November 2018].
- [40] C. Wang, N. Cao, J. Li, K. Ren and W. Lou, "Secure Ranked Keyword Search over Encrypted Cloud Data", in *International Conference on Distributed Computing Systems*, 2010. [41] V. Chang and M. Ramachandran, "Towards Achieving Data Security with the Cloud Computing Adoption Framework", *IEEE Transactions on Services Computing*, vol. 9, no. 1, pp. 138-151, 2016. Available: 10.1109/tsc.2015.2491281 [Accessed 31 January 2019].
- [42] A. Bhandari, A. Gupta and D. Das, "A framework for Data Security and Storage in Cloud Computing", in *International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT)*, 2016.
- [43] A. Youssef and M. Alageel, "A Framework for Secure Cloud Computing", *International Journal of Computer Science Issues (IJCSI)*, vol. 9, no. 4, 2012.
- [44] O. Mushtaq, F. Shahzad, O. Tariq, M. Riaz and B. Majeed, "An Efficient Framework for Information Security in Cloud Computing Using Auditing Algorithm Shell (AAS)", *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 14, no. 11, 2016.
- [45] H. Srivastava and S. Kumar, "Control Framework for Secure Cloud Computing", *Journal of Information Security*, vol. 06, no. 01, pp. 12-23, 2015. Available: 10.4236/jis.2015.61002.
- [46] S. Na, J. Park and E. Huh, "Personal cloud computing framework", in *IEEE Asia-Pacific Services Computing Conference*, 2011.
- [47] E. Endalew, "Cloud Data Security Framework for Payment Card System: the case of Ethiopia", MSc, Addis Ababa University: College of Natural Sciences, 2016.

- [48] X. Yan, X. Zhang, T. Chen, H. Zhao and X. Li, "The Research and Design of Cloud Computing Security Framework", Lecture Notes in Electrical Engineering, pp. 757-763, 2011. Available: 10.1007/978-3-642-25541-0_95.
- [49] F. Ellison and D. Parkhill, "The Challenge of the Computer Utility", OR, vol. 18, no. 3, p. 324, 1967. Available: 10.2307/3006988.
- [50] G. Briscoe and A. Marinou, "Digital Ecosystems in the Clouds: Towards Community Cloud Computing", in IEEE International Conference on Digital Ecosystems and Technologies, New York, USA, 2009, pp. 103-108.
- [51] ISACA. COBIT 5: A Business Framework for Governance and Management Enterprise IT., ISACA, 2012. Available at: <https://www.isaca.org/cobit>
- [52] W. Van Grembergen and S. De Haes, "IT Governance and its Mechanisms", in Proceedings of the 50th Hawaii International Conference on System Sciences, 2017.
- [53] A. Pandzo and K. Taljanovic, "IT Governance and IT Auditing Practice in Commercial Banks in Bosnia and Herzegovina", 2013, pp. 288-294.
- [54] ISO/IEC. ISO/IEC 27001:2013, ISO/IEC, Switzerland, 2013.
- [55] ITGI. COBIT 4.1. Rolling Meadows, Ill.: IT Governance Institute, 2007.
- [56] "ITIL Update | ITSM | AXELOS", Axelos.com, 2019. [Online]. Available: <https://www.axelos.com/itil-update>. [Accessed: 12- Mar- 2019].
- [57] ISO/IEC. ISO/IEC 20000-2:2005 Information technology — Service management — Part 1: Service management system requirements.
- [58] "2019 ITIL 4 Foundation - All Aspects of ITIL 4 Foundation", Master of Project Academy Blog, 2019. [Online]. Available: <https://blog.masterofproject.com/itil-v3-foundation/>. [Accessed: 13- Mar- 2019].
- [59] "Planning for and Implementing ISO 27001", Isaca.org. [Online]. Available: https://www.isaca.org/Journal/archives/2011/Volume-4/Pages/Planning-for-and-Implementing-ISO27001.aspx?utm_referrer=. [Accessed: 13- Mar- 2019].
- [60] S. Cots and M. Casadesús, "Exploring the service management standard ISO 20000", Total Quality Management & Business Excellence, vol. 26, no. 5, pp. 515-533, 2014. Available: 10.1080/14783363.2013.856544 [Accessed 20 March 2019].
- [61] ISO/IEC. ISO/IEC 38500: 2015 Corporate Governance of Information Technology. ISO/IEC, Geneva, Switzerland, 2015.
- [62] IAASB. ISAE 3402:2011 Assurance Reports on Controls at a Service Organization. IAASB, 2011.
- [63] D. Janvrin, E. Payne, P. Byrnes, G. Schneider and M. Curtis, "The Updated COSO Internal Control—Integrated Framework: Recommendations and Opportunities for Future Research", Journal of Information Systems, vol. 26, no. 2, pp. 189-213, 2012. Available: 10.2308/isis-50255.
- [64] P. Wood and D. Vickers, "Anticipated impact of the capability maturity model integration (CMMI®) V2.0 on aerospace systems safety and security", 2018 IEEE Aerospace Conference, 2018. Available: 10.1109/aero.2018.8396579.
- [65] Software Engineering Institute (SEI), "CMMI® for Services, Version 1.3", Carnegie Mellon University, 2010.
- [66] S. Godfrey, "Using CMMI for Improvement at GSFC", 2004.
- [67] L. Bloomberg and M. Volpe, Completing your qualitative dissertation. Los Angeles: Sage, 2012.
- [68] Y. Lin, N. Arshad, H. Haron, Y. Wah, M. Yusoff and A. Mohamed, "IT Governance Awareness and Practices: an Insight from Malaysian Senior Management Perspective", *Journal of Business Systems, Governance and Ethics*, vol. 5, no. 1, 2010. Available: 10.15209/jbsge.v5i1.177.
- [69] "Cloud Adoption Study," CIO Blog Spot, 2018. [Online]. Available: <https://blog.cionet.com/uploads/Cloud-Adoption-Survey>. [Accessed Feb 6 2018].
- [70] J. Creswell and D. Miller, "Determining Validity in Qualitative Inquiry", *Theory Into Practice*, vol. 39, no. 3, pp. 124-130, 2000. Available: 10.1207/s15430421tip3903_2.

Appendices

Appendix A: - Information Sheet

First of all, thank you for your time, consideration and willingness for helping me conduct this interview. My name is Obsa Taera, I am an MSc student in Computer Science at St. Mary's University. The title of my research is "Securing the Cloud through an IT Governance Framework".

Since the cloud environment is becoming widely adopted and at the same time users don't have full trust and confidence to use it since they transfer full control of their data to third-party cloud service providers, which hinders its applicability. Thus, the aim of this interview is to assess and understand the existing cloud services that are utilized by your organization and how you manage to secure these services and finally the information gathered is used to recommend an IT Governance framework that most suites the cloud computing environment by considering all the stakeholders engaged. Cloud service consumers and providers are going to benefit from this research since it makes the utilization of these services manageable and transparent for users.

Your cooperation in this interview is very much appreciated. The responses you give me will be very valuable for this research and will be used as an essential input for formulating the Cloud security framework. The information you provide me with will be kept confidential and only be used for academic purposes.

This interview takes approximately about 20-25 minutes to complete. As a participant of this interview, please note the following: if you seek any clarification on any of the questions you can ask me anything and you may withdraw from the interview at any time if you wish to and feel uncomfortable. Your responses will be kept absolutely confidential. The results collected from the interview will be used for the purposes of research only. Once again, thank you for your time and kind cooperation.

Yours sincerely,

Obsa Taera

Appendix B: - Consent Form

I, the undersigned have been informed that this interview is part of the study that explores the security of cloud computing. I have been told that the study will help develop a framework for improving cloud security and making it better adoptable and transparent for cloud service consumers. And also I have been told about the time it will take to complete the interview is approximately 20-25 minutes. Therefore, I am willing to participate in the study by signing this consent form.

The Study Participant's Name _____

Mobile Number _____

Date _____

The Study Participant's Signature _____

Interviewer Name _____

Appendix C: - Interview Guide

- 1) Tell me briefly about your organization? When it was established, what services do you give, number of staff, ...
- 2) Is there an IT department in your organization?
 - 2.1) How is your IT department structured? No. of IT staff?
- 3) Do you use any cloud services?
 - 3.1) What specific services? (IaaS, PaaS, SaaS or combination)
- 4) What kind of security controls are in place for the cloud services you provide/utilize?
 - 4.1) How do you manage the security of cloud services you use?
 - 4.2) Does your organization use an IT governance framework for cloud?
 - A. If yes, which framework?
 - B. If no, what difficulties do you face in not using such a framework?
- 5) What IT Governance framework do you use?
 - 5.1) How do you describe the level of IT governance framework enforcement in your organization?
 - 5.2) What challenges do you face in the implementation of the IT governance framework?
- 6) Is there any means of providing/getting performance measurement reports on the cloud service you use?
- 7) Do you think the cloud service you utilize is transparent?
- 8) Does the CSP introduce any third party related audits?
 - 8.1) If yes, are these audit reports available for customers on demand?
- 9) Have your organization signed SLA with the CSP?
 - 9.1) If yes, what are the focus areas in the SLA?
- 10) What recommendations do you have on the improvements of cloud security management?
- 11) What do you expect from the proposed framework?

Appendix D: - Support letter

ቅድስት ማርያም ዩኒቨርሲቲ
ድገረ-ምረቃ ት/ቤት



St. Mary's University
School of Graduate Studies

+251-11-552-45 37/66 ☒1211. 18490 Fax 552 83 49 e-mails: sgs@smuc.edu.et, Addis Ababa, Ethiopia

Ref.No. smusso/RP 0159/19

Date: - May 15, 2019

Request for Cooperation

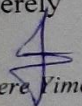
TO WHOM IT MAY CONCERN

Mr. **Obsa Taera**, ID No.SGS/0565/2009A is a graduate student in the department of **Computer Science**. He is working on his thesis entitled "**Securing the Cloud through IT Governance Framework**." and would like to collect data from your Organization.

Therefore, I kindly request your good office to allow him to access the data he needs for his research.

Any assistance rendered to him is highly appreciated.

Sincerely


Hamere Yimer

Guidance Counselor & Thesis Coordinator



Appendix E: - Meeting Minutes

Saturday, Feb 23rd, 2019 @ my office

Securing the Cloud through IT Governance Framework

ISAE 3402
 ISO 27001
 COBIT
 ISO 15-2005
 ISO/IEC 38500:2008
 ISO 17799
 ISO 20000

IT Governance Framework
 Cloud
 Insecurity
 PM
 Trust
 Comparative analysis
 Interview
 Non-Interview

more secure
 evaluation
 Related notes
 Summary
 Cloud-how?
 hole/gap
 IT Gover
 FW
 Table organization
 Experts Inputs
 Interview
 IT Officers

Proposed Framework

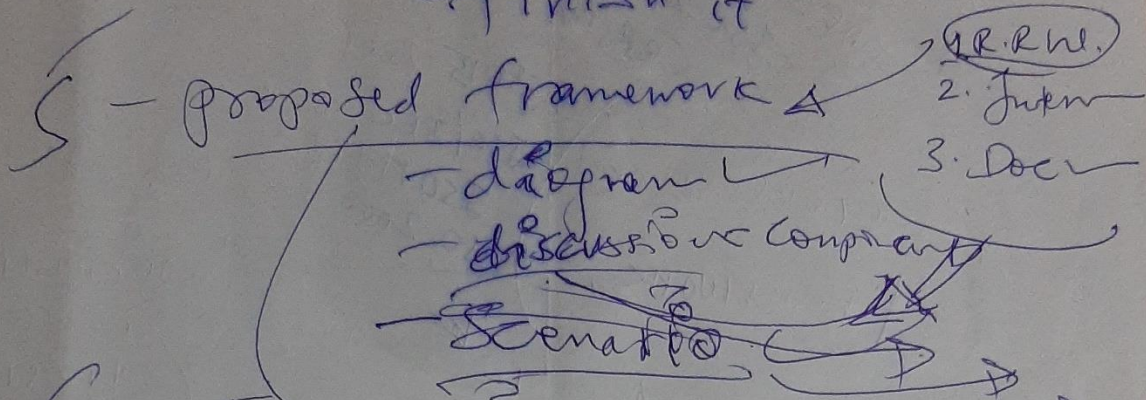
①

②

③

IT	Inputs	Interview

4 - Data Collection & Interpretation
finish it



6 - Evaluation (1) Against Interviewed

A) feedback (2) Non Interviewed

B) you 3p features vs

Features of system in the R.A.W.

7 - conclusions on JWS

