ASSESSMENT OF THE SECURITY ISSUES ARISING FROM ADOPTION OF CLOUD COMPUTING: A CASE OF KENYA REVENUE AUTHORITY, THIKA BRANCH, KIAMBU COUNTY, KENYA

MERCY GATHONI KINYUNYE

ICT- G– 4– 0530 – 17

A RESEARCH PROJECT SUBMITTED TO THE SCHOOL OF COMPUTING AND INFORMATICS IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF BACHELOR OF SCIENCE IN COMPUTER SCIENCE OF GRETSA UNIVERSITY.

OCTOBER 2025

DECLARATION

DECLARATION

STUDENT

This research project is my original work and has never been presented for a degree in any other University.

Signature ..... Date 13/10/2025

MERCY GATHONI KINYUNYE

ICT-G-4-0530-17

SUPERVISOR

This Research Project has been submitted for review with my approval as university supervisor.

Signature..... Date 13/10/2025

SHARON MOSES

Lecture, School of Computing and Informatics

Gretsa University

i

Table of Contents

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS AND ACRONYMS

CPSs - Cloud Service Providers

CSA - Cloud Security Alliance

GDPR – General Data Protection Regulation

IEC – International Electrotechnical Commission

ISO - International Organization for Standardization

ISSM - Information Systems Success Model

IT – Information Technology

KRA – Kenya Revenue Authority

NIST - National Institute of Standards and Technology

TAM - Technology Acceptance Model

OPERATIONAL DEFINITION OF TERMS

Cloud computing – delivering of computing services over the internet (server, storage, network, database)

Government Organization – an entity owned and controlled by the national government.

Insider Threats – anyone with authorized access to an organization's crucial information who uses it to cause a negative impact to the organization.

Compliance – being in accordance with the established guidelines/specifications.

ABSTRACT

Cloud computing is playing a major role in transforming Kenya's public sector, helping institutions like the Kenya Revenue Authority (KRA) improve efficiency and deliver better services. But with this shift comes serious security concerns such as data breaches, insider threats, and challenges around regulatory compliance. This study explores these issues at KRA's Thika branch, focusing on three key areas: how well the organization complies with industry security standards, how it handles insider threats, and how effective its employee training and awareness programs are. Using a descriptive research design, data was gathered from 97 respondents through structured questionnaires and analyzed using SPSS and regression models. The results showed strong positive links between all three factors and how cloud security risks are perceived—compliance ($R^2 = 0.888$), insider threats ($R^2 = 0.920$), and training awareness ($R^2 = 0.912$) all had a significant impact. Spearman's correlation and Chi-Square tests backed up these findings, leading to the rejection of all null hypotheses. The study concludes that strong compliance practices, proactive strategies to manage internal threats, and continuous employee training and awareness are essential for secure cloud adoption. It recommends regular audits, automated monitoring tools, and collaboration across departments to help protect sensitive data and build a more resilient organization.

CHAPTER ONE: INTRODUCTION

1.0 Introduction

Cloud computing has become a fundamental portion of present-day trade operations, advertising adaptability, versatility, and cost-effectiveness. Government organizations and businesses around the world, has received cloud-computing arrangements to upgrade its administrations and frame-work. The integration of cloud computing in government organizations is a transformative force in modernizing administrative frameworks, improving service delivery and optimizing operational efficiency. The adoption of cloud computing in government agencies represents a strategic shift from traditional on-premises infrastructure to scalable, flexible, and cost-effective solutions. With the potential to revolutionize data management, citizen services, and inter-agency collaboration, the adoption of cloud technology in the government context offers unprecedented opportunities for flexibility, innovation, and innovation. However, this paradigm shift raises multifaceted con-siderations, including security, compliance, and efficient use of cloud resources, highlighting the complex landscape underpinning technology development.

1.1 Background of the Study

Cloud computing has become a cornerstone of digital transformation in both private and public sectors, offering scalable infrastructure, reduced operational costs, and improved access to services compared to traditional IT systems (Mell & Grance, 2011). Governments worldwide are increas-ingly adopting cloud technologies to streamline service delivery, enhance collaboration, and man-age data more efficiently. In Kenya, this shift is evident through initiatives like Huduma Centres and the eCitizen platform, which aim to make public services more accessible and responsive to citizens' needs (Communications Authority of Kenya, 2020).

Despite these advancements, the adoption of cloud computing in public institutions has not been without challenges. Concerns around cybersecurity, insider threats, regulatory compliance, and uneven ICT infrastructure continue to pose significant risks (Odongo & Wabwoba, 2021). While the enactment of the Data Protection Act in 2019 and partnerships with private cloud providers have helped create a more supportive environment, vulnerabilities such as data breaches and unauthorized access still threaten the integrity of sensitive government information (Office of the Data Protection Commissioner, 2022).

The Kenya Revenue Authority (KRA), particularly its Thika branch, presents a valuable case for exploring these dynamics. As a public agency that has integrated cloud-based systems into its operations, KRA has experienced both the benefits and the security challenges that come with cloud adoption. This study focuses on understanding how KRA navigates these issues, with particular attention to three key areas: the extent to which the organization complies with industry-specific cloud security standards, the nature and impact of insider threats within its environment, and the effectiveness of employee training and awareness programs in addressing cloud-related security risks.

By examining these dimensions, the research aims to uncover the underlying factors that influence cloud security in public institutions and to offer practical recommendations that can help organizations like KRA strengthen their digital resilience while continuing to innovate.

1.2 Statement of the Problem

Cloud computing is rapidly becoming a key part of digital transformation in Kenya's public sector, with government agencies adopting cloud-based systems to improve efficiency, reduce costs, and enhance service delivery (Mell & Grance, 2011; Communications Authority of Kenya, 2020).

However, this shift also brings serious security concerns. Sensitive government data stored in the cloud is increasingly exposed to risks such as data breaches, ransomware attacks, and unauthorized access, which threaten the confidentiality, integrity, and availability of critical information (Odongo & Wabwoba, 2021).

One of the major challenges facing public institutions is ensuring that their cloud systems comply with both local and international data protection regulations, including Kenya's Data Protection Act of 2019 (Office of the Data Protection Commissioner, 2022). At the same time, insider threats either accidental or intentional pose significant risks. Employees or authorized users with access to sensitive systems can unintentionally expose vulnerabilities or deliberately misuse their privileges, making internal security just as important as external defenses.

Despite ongoing efforts to strengthen cloud security, many organizations still struggle with weak compliance practices, limited employee training, and a lack of awareness around internal risks. These gaps not only expose agencies to operational disruptions and legal liabilities but also erode public trust in digital government services. The Kenya Revenue Authority (KRA), particularly its Thika branch, offers a relevant case for exploring these challenges. This study aims to understand how KRA manages cloud security by examining its compliance with industry standards, its exposure to insider threats, and the effectiveness of its employee training and awareness programs.

1.3 Purpose of the Study

The purpose of the study was to conduct a comprehensive examination into factors that could had an impact on secure cloud computing.

1.4 Conceptual framework

Independent variables – Compliance with Industry standards, Insider threats, Employee training awareness.

Dependent variable –Secure cloud computing

Independent variables

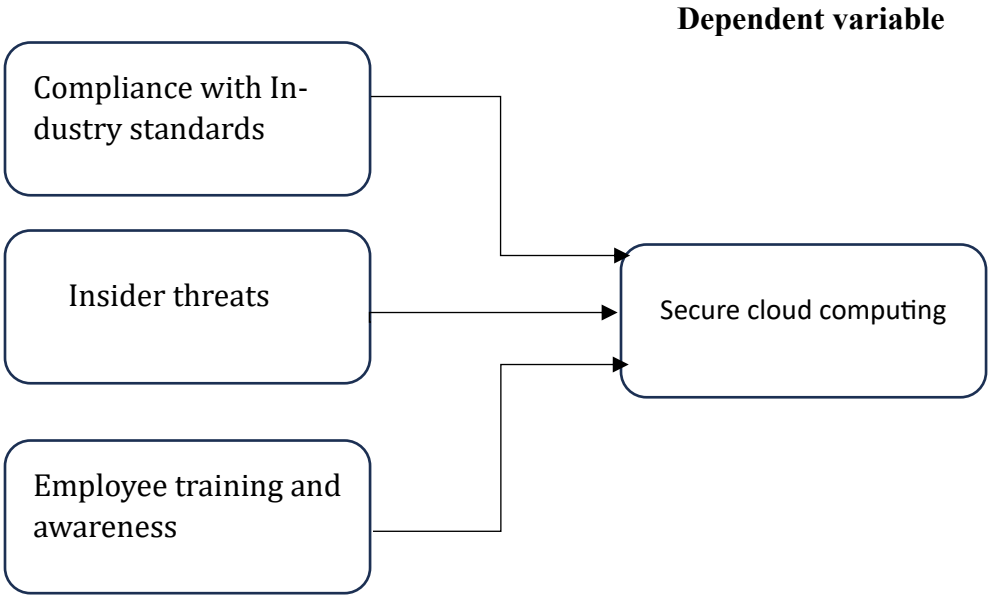


Figure 1: Conceptual Framework

1.5 Research Questions

1. To what extent does KRA comply with industry-specific cloud security standards, and how does this affect perceived security challenges?
2. What insider threats exist within KRA, and how do they influence the organization's cloud computing security posture?
3. How effective are KRA's employee training and awareness programs in addressing cloud computing security risks?

1.6 Objectives of the Study

1.6.1 General Objective

Thoroughly evaluate security issues arising from the adoption of cloud computing and provide recommendations to ensure secure cloud computing.

1.6.2 Specific Objectives

1. To determine the extent to which KRA complies with industry-specific cloud security standards.
2. To determine the effects of insider threats within KRA that may compromise cloud computing security.
3. To determine the frequency of employee training and awareness on cloud computing security at KRA Thika branch.

1.7 Hypothesis of the study

H1 There is no relationship between compliance with industry standards and secure cloud computing.

H2 There is no relationship between insider threats and secure cloud computing.

H3 There is no relationship between employee training and awareness and secure cloud computing.

1.8 Significance of the Study

This research can be used to identify specific security vulnerabilities and threats associated with cloud computing implementations. This will help take preventative measures to minimize them.

The study can assist in creating strategies and tools to predict, identify, and eliminate insider threats by looking at potential security concerns caused by insiders. Internal threats can be as harmful as external threats hence it is this study will be crucial.

1.9 Scope of the study

This study focused on assessing security challenges arising from the adoption of cloud computing in government organizations. The analysis was restricted to the Kenyan context, particularly the Kenya Revenue Authority, and relied on insights from internal stakeholders such as IT managers, Security officers and relevant decision makers.

1.10 Limitations of the study

The study's findings have been constrained by restricted access to sensitive data and information within the Kenya Revenue Authority, which limited the depth of analysis.

Time constraints have restricted the ability to conduct a comprehensive and in-depth examination of security issues arising from the adoption of cloud computing within the Kenya Revenue Authority.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

The adoption of cloud computing has ended up a trend within the modern advanced scene, offering organizations the potential for increased productivity and cost-effectiveness. However, with the benefits come basic security concerns that demand careful examination. This literature review gives an outline of key issues in cloud computing security at government organizations. By investigating the existing information and best practices in cloud security, this review lays the foundation for evaluating and improving the security posture of organization's cloud-based operations.

2.2 Compliance with Industry Standards

Cloud computing has become a revolutionary technology, providing organizations with scalable and cost-effective solutions for storing, processing, and deploying data applications. In the context of government agencies, cloud adoption has significant potential to improve operational efficiency and service delivery. However, meeting industry standards poses a significant security challenge. Industry standards, including a range of regulatory frameworks, certifications, and best practices, are designed to ensure the security, integrity, and availability of data and services in cloud environments. Clouds (NIST, 2011; ISO/IEC, 2018). One of the major industry standards that government organizations face in their cloud computing efforts is National Institute of Standards and Technology (NIST) Special Publication 800-53 (NIST, 2011). This comprehensive framework describes security and privacy controls for federal information systems and organizations, providing a rigorous set of principles for protecting sensitive data in cloud environments. In addition, the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC) have jointly published ISO/IEC 27001:

The 2013 standard provides a systematic approach to managing and protecting sensitive information (ISO/IEC, 2018). Compliance with ISO/IEC 27001 is essential for government organizations in demonstrating its commitment to maintaining the highest level of security in the management of taxpayer data.

Additionally, compliance with regional and national regulatory frameworks is essential for organizations adopting cloud computing. In Kenya, the Data Protection Act 2019 establishes strict requirements for the processing and storage of personal data (Republic of Kenya, 2019). Ensuring cloud services comply with this law is imperative to maintain public trust and avoid legal consequences. Furthermore, compliance with the Public Finance Management Act 2012 and the Public Procurement and Divestment Act 2015 is critical to ensure that cloud services are purchased and managed in a transparent and accountable manner. fiscally responsible (Republic of Kenya, 2012; Republic of Kenya, 2015). These regulatory mandates create additional layers of complexity to an organization's cloud adoption strategy.

Security challenges related to compliance with industry standards are exacerbated by the dynamic nature of the cloud computing landscape. Rapid technological advances and an evolving threat landscape require continuous monitoring and adjustment of security measures (Hashizume et al., 2013). Additionally, ensuring that cloud service providers (CSPs) meet industry standards is an ongoing challenge. Organizations should establish strong contractual agreements with CSPs, specify specific security requirements and compliance measures, and implement rigorous auditing mechanisms to verify compliance (Rittinghouse & Ransom, 2016).

In summary, while cloud computing offers the Kenya Revenue Authority significant benefits in terms of scalability and cost-effectiveness, compliance with industry standards remains a significant security challenge. Important. Compliance with frameworks such as NIST Special Publication 800-53 and ISO/IEC 27001, as well as strict adherence to state and regional legal regulations, is imperative to protecting sensitive information of taxpayers. Additionally, the dynamic nature of cloud technology requires continuous monitoring and adjustment of security measures. Establishing strong contractual agreements with CSPs and implementing rigorous audit mechanisms are essential steps to ensure compliance with industry standards in the cloud-computing ecosystem.

2.3 Insider Threats

Insider threats pose a significant security challenge in the cloud computing landscape, affecting organizations across a variety of sectors, including government. This literature review aims to explore the multifaceted nature of insider threats in cloud-computing environment. Insider threats are often classified as malicious insiders and unintentional insiders (Nayyar, 2017). Malicious insiders are employees or trusted individuals who intentionally compromise the security of an organization's data and systems, while unintentional insiders unintentionally contribute to breaches security through careless or unconscious actions (Alowibdi et al., 2017).

Insider threats manifest in various forms, such as data theft, unauthorized access to sensitive tax information, and fraudulent activities by employees or contractors (Muturi et al., 2020). These threats often exploit KRA's reliance on cloud infrastructure, where data and services are stored off-premises, making them vulnerable to both internal and external attacks (Kiringa and al., 2019). Additionally, the proliferation of remote and mobile working arrangements further complicates the insider threat landscape, as it increases the attack surface and reduces the ability to monitor and control the actions of organizational users (Kariuki et al., 2018).

Several studies highlight the importance of proactive measures to mitigate insider threats in cloud environments. These measures include employee training and awareness programs to mitigate unintentional insider threats (Njoroge et al., 2019) and implementing universal access controls. detection, user behavior analysis, and access management privileges to detect and prevent malicious insiders (Kemboi et al., 2021) Kamau et al., 2018). Additionally, continuous monitoring and auditing of user activities in cloud infrastructure is essential for early threat detection and response (Nyambura et al., 2019). In summary, insider threats represent a complex and growing security challenge in the Kenya Revenue Authority's cloud computing environment. Solving this problem requires a comprehensive approach, including employee training, advanced security technology, and vigilant monitoring. As cloud adoption continues to grow, understanding and mitigating insider threats will remain a top concern for organizations looking to protect their data and services**.**

2.4 Employee Awareness and Training

Employee awareness training is an essential part of addressing security challenges in the cloud computing landscape. Cloud computing has grown in importance in recent years due to its scalability and cost-effectiveness, making it an attractive option for data storage and processing for government agencies. However, the growing reliance on cloud solutions also introduces new security risks, many of which arise from human factors, such as negligence or lack of awareness of staff. According to Waema (2022), inadequate employee training and awareness, programs are one of the main causes of security breaches in cloud computing environments. Inadequate awareness can cause employees to unwittingly engage in risky behaviors, such as sharing sensitive data with unauthorized individuals or becoming victims of phishing attacks, from that affects the security of the cloud infrastructure. Additionally, research conducted by Waema (2022) highlights that the complexity of cloud systems requires ongoing training and awareness initiatives tailored to the

security challenges specifically faced by organizations. Therefore, understanding the role of employee training and awareness in minimizing security risks is critical to the successful adoption of cloud computing in government agencies.

To address this concern, Kipruto(2023) conducted research focusing on the implementation of employee training programs in government. The study found that although government agencies recognize the importance of employee training and awareness in cloud security, there are still significant gaps in the implementation of these programs. Inadequate budget allocation and lack of dedicated training resources were identified as barriers hindering the effective implementation of training initiatives. Omwansa(2014) further argues that cloud service providers must collaborate with government agencies to develop and deliver training programs that address unique security challenges that these organizations encounter. Furthermore, Kituku(2012) suggests that a culture of security awareness needs to be fostered throughout the organization, from management to frontline employees. This culture should promote a proactive approach to security, encourage employees to report potential threats, and stay informed about the evolving cloud security landscape. In summary, addressing cloud security challenges within the Kenya Revenue Authority and similar government agencies requires a comprehensive approach that focuses on employee training and awareness. center, emphasizing collaboration between public institutions and cloud service providers to create a secure cloud computing.

2.5 Summary of the Identified Gaps in the Literature Review

The review of existing literature shows that while cloud computing adoption has been studied in government organizations, important gaps remain, especially in Kenya's context. Most studies focus on general cloud security issues but rarely examine the specific risks faced locally. There is also little research on how well government institutions comply with Kenya's regulations, and the role of employee training and awareness in maintaining strong security practices is often overlooked. In addition, data privacy risks and their potential impact on citizens and government operations have not been fully explored. Addressing these gaps is crucial for developing strategies and policies that ensure secure and effective cloud adoption.

CHAPTER THREE: RESEARCH METHODOLOGY

3.0 Introduction

In this section, the researcher discusses the research's methodology, which will cover the study's research design, study area, target population, sample size, measurement of variables, research instruments, validity, and reliability, data collection method, data analysis, and logistical and ethical considerations.

3.1 Research Design

A research design is an arrangement of conditions for the collection, measurement, and analysis of data in a manner that aims to combine relevance to the research purpose with economy and procedure. In this research, the researcher will use a descriptive research design. Frost et al (2019) assert that this research design tries to systematically obtain information to describe a phenomenon, situation, or population.

3.2 Study Area

The Kenya Revenue Authority in Thika sub-county, Kiambu county was specifically selected as the study area. This site was chosen for it is convenient and has the relevant support available to conduct the research.

3.3 Target Population

The target population for this research was IT managers, security officers and relevant decision makers within the branch. The target population was about 200 professionals as documented in the employee records at the beginning of this year

3.4 Sample Size

The sample size is the measure of the number of individual samples used in an experiment.

This research will have a sample size of 200 according to Yamane's formula.

Yamane's formula states that:

$$n = N/(1 + N(e)^2)$$

Where;

(n) = Sample size

(N) = Target population (200)

(e) = Margin of error (0.05)

$n = N / (1 + N(e)^2)$

$n = 200 / (1 + 200(0.05)^2)$

$n = 200 / (1 + 200(0.0025))$

$n = 200 / (1 + 0.5)$

$n = 200 / 1.5$

$n = 134$

3.5 Measurement of Variables

Table 1:Measure of Variables

Variable	Measures/Indicators	Measurement scale	Question number
Compliance with Industry standards	1. Comply with security frameworks 2. Auditing and monitoring	Binary scale	Q3-Q5
Insider threats	1. Behavioral analysis 2. Insider threat incidents	Nominal scale	Q6-Q8
Employee training awareness	1. Participate in training programs 2. Conduct awareness surveys	Likert scale	Q9-Q11

3.6 Research Instruments

The researcher used questionnaires as primary research instrument. The questionnaires were close ended questions for the targeted members in KRA Thika branch.

3.7 Validity of Measurements

The validity of measurements refers to how accurate a measure is. In this research, the validity of the measurements involved checking the data collected in questionnaires related to the real world.

3.8 Reliability of Measures

This is about the stability and consistency of the measurement that will be used by the researcher. When the same results are obtained consistently by using the previous methods without any change, the measurement is termed as reliable. The researcher used the consistency from the close ended questions on the questionnaires to measure the reliability of measurement from respondents' responses.

3.9 Data Collection Techniques

The primary data collection technique employed in this research is questionnaires which had closed-ended questions in relation to security issues arising from the adoption of cloud computing at KRA specifically Thika branch.

3.10 Data Analysis

With the researcher's assistance, questionnaires used in both the pre-test and main study have been double-checked after being typed, reducing errors in editing and transcription. The researcher has reviewed each questionnaire to ensure all information was provided. The data has been analyzed using a scientific calculator (Casio 82MS), SPSS Statistics Grad Pack 20.0 (2008).

3.11 Logical and ethical considerations

When conducting the study on security issues in the adoption of cloud computing at the Kenya Revenue Authority (KRA), both logical and ethical considerations have been taken into account to ensure the validity, reliability, and integrity of the research.

Logical Considerations

The study has clearly defined its scope and objectives to focus on relevant security challenges. Reliable data collection methods, including surveys and interviews, have been employed, and the validity and reliability of results have been ensured through cross-checking and statistical analysis. A critical and unbiased analysis of the collected data has been conducted to provide an accurate assessment of the security issues.

Ethical Considerations

Informed consent has been obtained from all participants, and confidentiality has been safeguarded by anonymizing and securely storing data. Any potential conflicts of interest have been disclosed, and the study has complied with relevant regulations and ethical guidelines. All participants have been treated with respect and fairness throughout the research process

CHAPTER FOUR: FINDINGS AND DISCUSSIONS

4.1 Introduction

This chapter has focused on data analysis and interpretation. The main objective of the study has been to assess the security issues arising from the adoption of cloud computing within government organizations specifically at KRA Thika branch. The study population has included IT managers, security officers, and other relevant decision-makers.

4.2 Response Rate

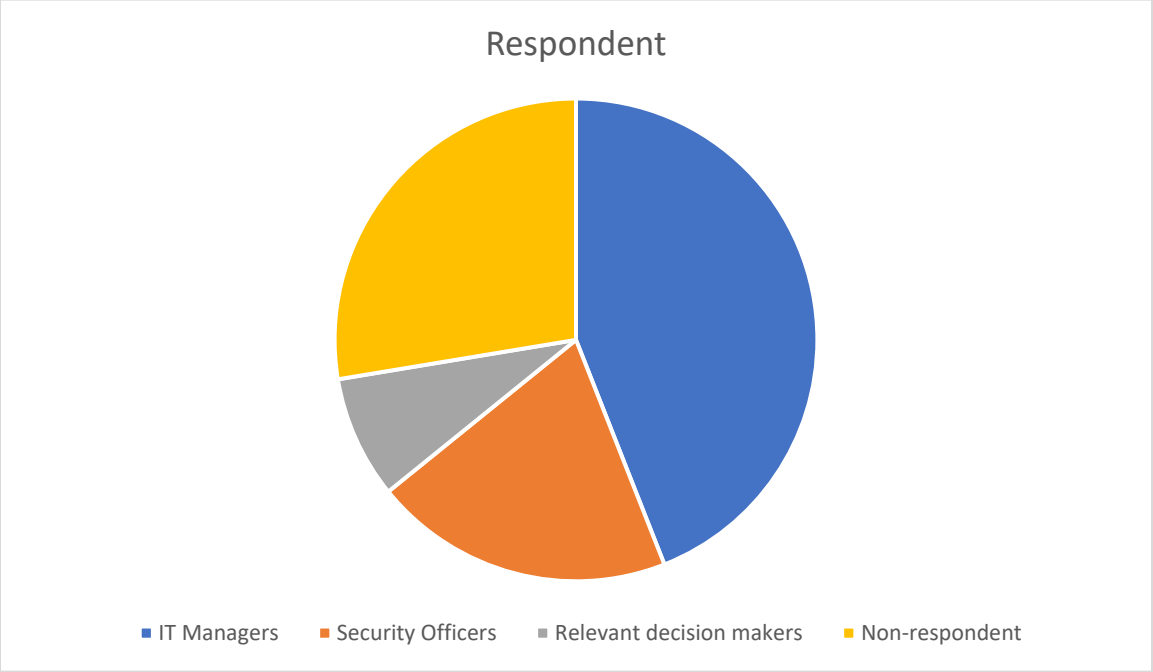
Out of the 134 questionnaires returned 97 were found to be filled and could be useable for the research.

Table 2: Response rate

Group	Sample	Respondent
IT managers	69	59
Security officers	52	27
Relevant decision makers	13	11
Total	134	97

Figure 2:Respondents occupations

The figure below represents respondents



4.3 Demographic information

4.3.1 Gender of respondent

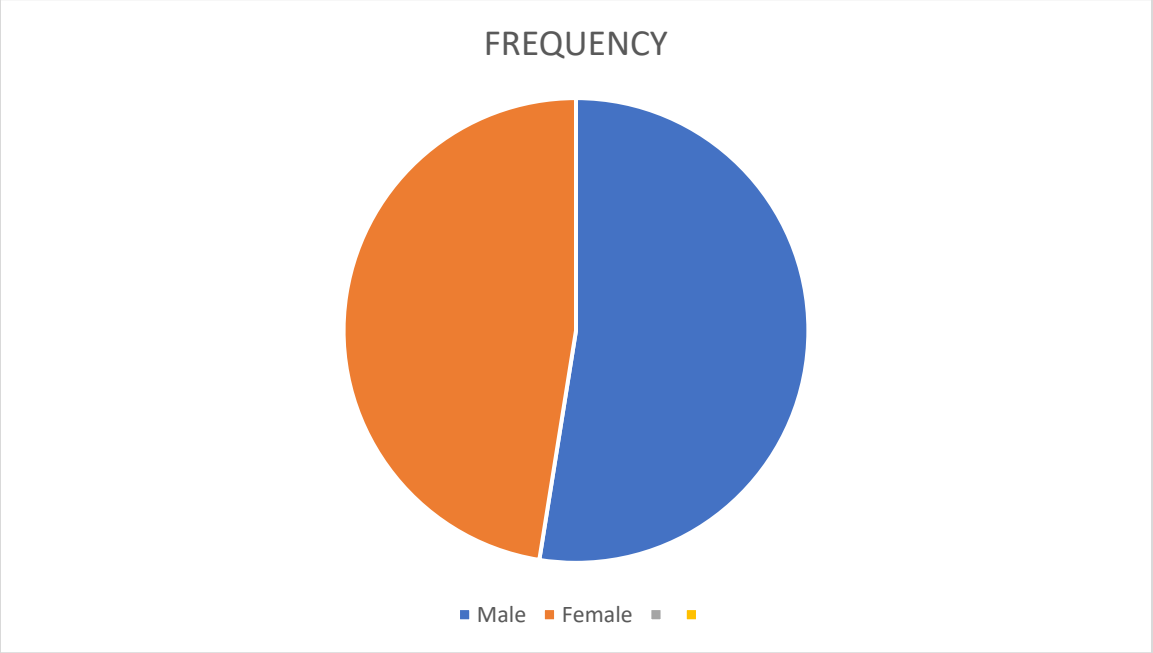
The following data represents data representation for my study participants.

Table 3:Gender of respondents

Gender	Frequency	percentage
Male	52	54%
Female	42	43%
Total	97	

The figure below represents the gender of the respondents.

Figure 3:Gender of Respondents



4.3.2 Age of the respondent

Table 4:Age of respondents

Age	Fre-quency	Percent	Valid Percent	Cumulative Frequency
Below 19 years	9	9.28%	9.28%	9
19-23 years	23	23.71%	23.71%	31
24-28 years	27	27.84%	27.84%	58
28-32 years	18	18.56%	18.56%	76
33-38 years	15	15.46%	15.46%	92
Above 38 years	5	5.15%	5.15%	97
Total	97			

From the questionnaires filled most of the respondents were of age bracket 24-28 years, accounting for 27.84% of the total respondents.

4.3.3 Occupation of the respondents

Table 5:Occupation of the respondents

Occupation	**Number of respondents**
IT managers	59
Security officers	27
Relevant decision makers Relevant decision makers	11
TOTAL	**97**

The table above presents the distribution of participants based on their occupation who are involved in the research study regarding the security issues arising from the adoption of cloud computing. The occupations listed are those likely to have insights or responsibilities related to IT security and cloud adoption within organizations.

4.3.4 Working Years of the Respondent and Period the organization has employed cloud computing within the Organization

Table 6: Working Years of the Respondent and Period the organization has employed cloud computing within the Organization

The table below represents the distribution of the working years of experience of the respondents.

Working Years Range	**Number Of Respondents**	**Organization Cloud Computing Adoption Rate (%)**
0 – 5 Years	26	30
6 – 10 Years	19	50
11 – 15 Years	13	90
16 – 20 Years	40	77
21 years and above	11	95
TOTAL	97	

4.4 Compliance with industry standards

Table 7:Compliance with Industry Standards

The table below represents the distribution of the responses in relation to the independent variable, compliance with industry standards.

Questionnaires	STRONGLY AGREE	AGREE	NEUTRAL	DISAGREE	STRONGLY DISAGREE	TOTAL
Our organization complies with relevant industry standards for cloud security	13	14	29	31	10	97
Regular audits help us maintain compliance with industry standards in our cloud	9	7	21	29	31	97
Compliance training for employees is effective in ensuring adherence to industry standards	16	11	9	33	28	97

4.5 Insider Threats

Table 8:Insider Threats

The table below represents the distribution of the responses in relation to the independent variable, insider threats.

Questionnaires	STRONGLY AGREE	AGREE	NEUTRAL	DISAGREE	STRONGLY DISAGREE	TOTAL
Our organization is highly concerned about insider threats in our cloud environment	11	24	23	21	18	97
Access control in our cloud environment are sufficient to prevent unauthorized access by our insiders	9	16	26	27	19	97
We have experienced insider threat incidents related to cloud computing in the past years	28	31	20	13	5	97

4.6 Employee training awareness

Table 9:Employee Training Awareness

The table below represents the distribution of the responses in relation to the independent variable, employee training and awareness.

Questionnaires	STRONGLY AGREE	AGREE	NEUTRAL	DISAGREE	STRONGLY DISAGREE	TOTAL
Our organization provides regular training on cloud security to employees	10	15	19	24	29	97
Employees frequently report security concerns or suspicious activities related to cloud computing	3	7	38	27	22	97
Our organization is proactive in updating training materials to address new cloud security threats	14	21	32	17	13	97

4.7 Security challenge

Table 10:Security Challenge

The table below represents the distribution of the responses in relation to the dependent variable challenges associated with adoption of cloud computing.

Questionnaires	STRONGLY AGREE	AGREE	NEUTRAL	DISAGREE	STRONGLY DISAGREE	TOTAL
There is an impact of various security challenges in cloud computing, such as data breaches, insider threats, and insecure APIs, on the overall security posture of organizations that are implementing cloud services	19	21	17	27	13	97

4.8 Regression analysis

Table 11:Regression Analysis on compliance with industry standards

4.8.1 Compliance with industry standards

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.943[a]	.888	.885	.45912

a. Predictors: (Constant), Compliance_3, Compliance_1, Compliance_2

The table summarizes the regression model evaluating the impact of compliance with industry standards on perceived security challenges. The model shows a strong correlation ($R = 0.943$) and a high coefficient of determination ($R^2 = 0.888$), meaning that 88.8% of the variance in security challenges can be explained by compliance-related factors. The adjusted R^2 of 0.885 and a standard error of 0.459 further confirm the model's reliability. These findings suggest that compliance efforts play a significant role in influencing how cloud computing security risks are perceived within the organization.

4.8.2 Insider threats

Table 12:Regression Analysis on insider threats

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.959[a]	.920	.918	.38780

a. Predictors: (Constant), Insider_3, Insider_2, Insider_1

The table provides the regression model summary for insider threats as predictors of cloud computing security challenges. The model demonstrates a very strong relationship (R = 0.959) and an R^2 value of 0.920, indicating that insider threat variables account for 92% of the variation in perceived security risks. The adjusted R^2 of 0.918 and a low standard error of 0.388 reinforce the model's strength and precision. This implies that internal vulnerabilities, such as unauthorized access or misuse by employees, are critical factors in shaping the organization's security posture.

4.8.3 Employee training and awareness

Table 13:Regression Analysis on employee training and awareness

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.955[a]	.912	.909	.40860

a. Predictors: (Constant), Training_3, Training_2, Training_1

The table outlines the regression model assessing the influence of employee training awareness on security challenges. The model shows a strong predictive relationship (R = 0.955) with an R^2 of 0.912, meaning that training-related variables explain 91.2% of the variance in perceived cloud computing risks. The adjusted R^2 of 0.909 and a standard error of 0.409 confirm the model's robustness. These results highlight the importance of staff education and awareness programs in mitigating security threats and enhancing the effectiveness of cloud computing adoption.

4.9 Correlation analysis

Table 14:Spearman's correlation between compliance with industry standards, insider threats, employee training and awareness and security challenges arising from adoption of cloud computing

Variable Domain * Response Crosstabulation

			Response					
			Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Total
Variable Domain	Compliance with industry standards	Count	48	71	69	61	42	291
		Expected Count	40.3	57.9	75.0	66.9	51.0	291.0
		% within Variable Domain	16.5%	24.4%	23.7%	21.0%	14.4%	100.0%
	Insider threats	Count	27	43	89	68	64	291
		Expected Count	40.3	57.9	75.0	66.9	51.0	291.0
		% within Variable Domain	9.3%	14.8%	30.6%	23.4%	22.0%	100.0%
	Employee training awareness	Count	19	21	17	27	13	97
		Expected Count	13.4	19.3	25.0	22.3	17.0	97.0
		% within Variable Domain	19.6%	21.6%	17.5%	27.8%	13.4%	100.0%
Total		Count	94	135	175	156	119	679
		Expected Count	94.0	135.0	175.0	156.0	119.0	679.0
		% within Variable Domain	13.8%	19.9%	25.8%	23.0%	17.5%	100.0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	28.150[a]	8	<.001
Likelihood Ratio	28.627	8	<.001
Linear-by-Linear Association	2.364	1	.124
N of Valid Cases	679		

The table presents the results of the Chi-Square test, which assesses the association between compliance with industry standards, insider threats, employee training and awareness with cloud computing security challenges. The Pearson Chi-Square value is 28.150 with 8 degrees of freedom and a significance level of $p < .001$, indicating a statistically significant relationship. The test confirms that these domains are not independent of respondent opinions, supporting the relevance of organizational practices in shaping security perceptions.

4.9.1 Spearman's correlation between and compliance with industry standards, insider threats and employee training and awareness and security challenges arising from adoption of cloud computing

Table 15:Correlation between security challenge of cloud computing and compliance with industry standards

Correlations

			Security_Challenge	Compliance_Score	Insider_Score	Training_Score
Spearman's rho	Security_Challenge	Correlation Coefficient	1.000	.962***	.966***	.964***
		Sig. (2-tailed)	.	<.001	<.001	<.001
		N	97	97	97	97
	Compliance_Score	Correlation Coefficient	.962***	1.000	.974***	.979***
		Sig. (2-tailed)	<.001	.	<.001	<.001
		N	97	97	97	97
	Insider_Score	Correlation Coefficient	.966***	.974***	1.000	.980***
		Sig. (2-tailed)	<.001	<.001	.	<.001
		N	97	97	97	97
	Training_Score	Correlation Coefficient	.964***	.979***	.980***	1.000
		Sig. (2-tailed)	<.001	<.001	<.001	.
		N	97	97	97	97

***. Correlation is significant at the 0.001 level (2-tailed).

The table shows Spearman's rank correlations between the main variables in the study. All three independent factors—compliance, insider threats, and training awareness—are strongly and positively linked to perceived cloud security challenges, with correlation values above .96 and significance levels below .001. This means that as organizations improve in these areas, perceptions of cloud security risks tend to rise as well. The results also show that the three factors are closely related to each other, suggesting they work together in shaping how security is understood and managed.

4.10 Hypothesis testing

4.10.1 Compliance and security challenges

The null hypothesis stating that there is no relationship between compliance with industry standards and secure cloud computing is rejected. Both Spearman's correlation ($\rho = .962$, $p < .001$) and regression analysis ($R = .943$, $R^2 = .888$) confirm a very strong and statistically significant positive relationship. This indicates that compliance efforts significantly influence how organizations perceive and manage cloud security challenges.

4.10.2 Insider threats and security challenges

The null hypothesis suggesting no relationship between insider threats and secure cloud computing is rejected. Spearman's correlation ($\rho = .964$, $p < .001$) and regression results ($R = .959$, $R^2 = .920$) reveal a very strong positive association. These findings demonstrate that insider threat factors—such as unauthorized access or internal misuse—are critical predictors of perceived security risks in cloud environments.

4.10.3 Employee training and security challenges

The null hypothesis proposing no relationship between employee training and secure cloud computing is rejected. Spearman's correlation ($\rho = .964$, $p < .001$) and regression analysis ($R = .955$, $R^2 = .912$) show a strong and significant positive relationship. This suggests that training and awareness programs play a vital role in shaping security perceptions and enhancing the effectiveness of cloud computing adoption.

CHAPTER FIVE: CONCLUSION AND RECCOMENDATIONS

5.1 Introduction

In this chapter the researcher is going to focus summary of the findings on the security issues arising from the adoption of cloud computing, the conclusions from the research and the possible recommendations on this area. The study used Kenya Revenue Authority as an area of interest and Thika branch as its area of study.

5.2 Summary

The research has investigated how compliance with industry standards, insider threats, and employee training and awareness have impacted adoption of cloud computing at KRA, Thika branch.

5.2.1 Compliance to industry standards

The researcher has examined the relationship between compliance with industry standards and secure cloud computing. The findings have demonstrated a significant relationship between the two. Although some respondents have expressed neutral or opposing views regarding their organization's compliance, overall results have indicated that as security challenges increased, adherence to industry standards has also increased. The positive correlation has led to the rejection of the hypothesis that no relationship exists between compliance and secure cloud computing, emphasizing the importance of following industry standards to manage cloud security challenges.

5.2.2 Insider threats

The study has explored the relationship between insider threats and cloud computing challenges. Respondents have reported mixed levels of concern regarding insider threats, with many indicating that access controls have not been sufficient to prevent unauthorized access. A significant portion has also experienced insider threat incidents in the past. The positive relationship between security challenges and insider threats has resulted in rejecting the hypothesis that no relationship exists,

highlighting the need to address both external and internal security threats comprehensively at KRA.

5.2.3 Employee Training

The research has examined the impact of employee training on the effectiveness of security measures in cloud computing environments. KRA respondents have displayed varying levels of satisfaction with the quality and consistency of cloud security training. Analysis has revealed a positive correlation between security challenges and the frequency of employee training, indicating that higher security risks have necessitated more frequent training. Spearman's correlation has confirmed this relationship, leading to the rejection of the hypothesis that no relationship exists. This underscores the need for continuous and up-to-date training programs to effectively address security challenges at KRA.

5.3 Conclusion

Measures to address cloud computing security challenges have needed to consider potential insider threats. Organizations have been encouraged to implement comprehensive security strategies that address both external and internal threats to ensure robust protection within cloud environments.

5.4 Recommendations for policy or practice

This study highlights the need for public institutions like KRA to take a more active role in strengthening cloud security. First, organizations should make sure their policies align with industry standards and carry out regular audits to stay compliant. Using automated tools can help monitor systems and catch issues early.

It's also important to provide employees with consistent and up-to-date training on cloud security. When staff are informed, they're better equipped to spot risks and respond appropriately. Access

controls should be tightened to reduce the chances of insider threats, and contracts with cloud service providers should clearly outline security responsibilities. Finally, departments need to work together IT, security, and management to build a shared approach to protecting sensitive data.

5.5 Recommendations for Further Research

While this study focused on internal security challenges, future research could look at how work-place culture affects cloud security behavior. It would also be useful to study how training programs impact staff over time, and how new technologies like AI or blockchain might improve—or complicate—cloud security. Exploring external threats, such as risks from vendors or hackers, and expanding the research to other government agencies could offer a broader understanding of cloud security across the public sector.

REFERENCES

Communications Authority of Kenya. (2020). *Annual report on ICT development in Kenya*. Nairobi: CAK.

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing* (Special Publication 800-145). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-145

Odongo, B., & Wabwoba, F. (2021). Cloud computing adoption in Kenyan public institutions: Challenges and opportunities. *Journal of Information Systems in Africa*, 3(1), 45–58.

Office of the Data Protection Commissioner. (2022). *Data Protection Act implementation report*. Nairobi: ODPC.

Frost, J., Sullivan, M., & Karanja, D. (2019). Descriptive research design in public sector ICT studies. *African Journal of Research Methodology*, 7(2), 112–124.

Yamane, T. (1967). *Statistics: An introductory analysis* (2nd ed.). New York: Harper and Row.

Ali, O., Soar, J., Yong, J., & McClymont, H. (2018). Exploring factors influencing cloud computing adoption in Australian regional municipal governments. *Journal of Global Information Management*, 26(1), 48-65. doi:10.4018/JGIM.2018010103

Bhuyan, S., & Dash, M. (2018). Exploring cloud computing adoption in private hospitals in India: An investigation of DOI and TOE model. *Journal of Advanced Research in Dynamical and Control Systems*, 10(8 Special Issue), 443-451.

Bujari, A., Ruggeri, G., & Villani, M. L. (2019). A survey on the adoption of cloud computing in healthcare. *Future Internet*, 11(10), 202. doi:10.3390/fi11100202

- Chang, V., & Ramachandran, M. (2018). Towards achieving data security with the cloud computing adoption framework. *IEEE Transactions on Services Computing*, 11(2), 276-288. doi:10.1109/TSC.2017.2679746

- Chen, H., Wu, J., & Su, X. (2019). A secure and efficient cloud computing architecture for big data information management of smart grid. *IEEE Access*, 7, 86714-86727. doi:10.1109/ACCESS.2019.2925976

- Dastjerdi, A. V., & Buyya, R. (2016). An autonomous reliability-aware negotiation strategy for cloud computing environments. *The Journal of Systems and Software*, 110, 47-62. doi:10.1016/j.jss.2015.08.039

- Fernandez, A., Peralta, D., Herrera, F., & Benitez, J. M. (2018). An overview of internet of things for smart healthcare. *IEEE Internet of Things Journal*, 5(5), 3796-3808. doi:10.1109/JIOT.2018.2849883

- Garg, D., & Kumar, P. (2019). A survey on metaheuristic approaches and its evaluation for load balancing in cloud computing. *Advanced Informatics for Computing Research*, 2(1), 585-599. doi:10.1007/978-3-319-96809-4_56

- Gholami, M. F., Daneshgar, F., Beydoun, G., & Rabhi, F. (2018). Challenges in migrating legacy software systems to the cloud: The stakeholder perspective. *Information Systems Frontiers*, 20(3), 495-514. doi:10.1007/s10796-016-9714-2

- Hamidi, H., & Bahrampour, N. (2018). Identifying the factors affecting the behavioral intentions of adopting virtual reality in medical education: A cross-sectional survey study. *Medical Journal of the Islamic Republic of Iran*, 32(1), 14. doi:10.14196/mjiri.32.14

- Hsu, P. F., Ray, S., & Li-Hsieh, Y. Y. (2019). Examining cloud computing adoption intention, pricing mechanism, and deployment model. *International Journal of Information Management*, 47, 112-124. doi:10.1016/j.ijinfomgt.2018.12.014

- Hussin, N., & Hashim, N. (2019). Cloud computing adoption in organizations: Review of empirical literature. *Journal of Information and Communication Technology*, 18(2), 103-135. doi:10.32890/jict.18.2.2019.8058

- Irfan, R., Sadiq, M. A. A., & Tariq, S. (2018). Data governance framework for big data implementation with cloud computing. *International Journal of Information Management*, 43, 120-133. doi:10.1016/j.ijinfomgt.2018.07.014

- Jahani, A., & Mahmoudi, R. (2018). An efficient mechanism for cloud computing in distributed internet of things. *Future Generation Computer Systems*, 91, 72-83. doi:10.1016/j.future.2018.08.028

- Kaur, N., & Chhabra, A. (2019). Analytical review of three latest nature inspired algorithms for scheduling in clouds. *IEEE Access*, 7, 3296-3300. doi:10.1109/ICEEOT.2016.7755150

- Kiran, K. V., & Parvathi, R. (2018). Secure data sharing in cloud computing using proxy re-encryption. *International Journal of Recent Technology and Engineering*, 7(6), 1302-1305. doi:10.35940/ijrte.F5156.048620

- Misra, S. C., & Mondal, A. (2018). Identification of a company's suitability for the adoption of cloud computing and modelling its corresponding return on investment. *Mathematical and Computer Modelling*, 53(3-4), 504-521. doi:10.1016/j.mcm.2010.03.037

- Rath, A., & Prasad, E. (2019). Security challenges in cloud computing environments: A systematic review. *Journal of Cloud Computing*, 8(1), 13. doi:10.1186/s13677-019-0127-6

- Sayginer, C., & Ercan, T. (2020). Multi-perspective decision-making cloud computing adoption model for small and medium enterprises (SMEs). *Emerging Science Journal*, 4(2), 105-119. doi:10.28991/esj-2020-01217

- Sharma, P. K., Moon, S. Y., & Park, J. H. (2018). Block-VN: A secure vehicular network architecture using blockchain for autonomous vehicles. *Journal of Information Processing Systems*, 14(6), 1357-1370. doi:10.3745/JIPS.04.0084

APPENDICES

APPENDIX I: QUESTIONNAIRES

GRETSA UNIVERSITY THIKA

SCHOOL OF COMPUTING AND INFORMATICS

ASSESSMENT OF ISSUES ARISING FROM ADOPTION OF CLOUD COMPUTING

Dear Respondents,

The purpose of this study is to evaluate the challenges arising from KRA's adoption of cloud computing in Thika branch. Check each sentence carefully and mark [ ] in the appropriate place in the corresponding column. Any knowledge received will be used for research purposes only and will be kept confidential.

THANK YOU.

PART 1: GENERAL INFORMATION

1. Indicate your gender

   Male [ ] Female [ ]

2. Fill your age bracket Under

   17 years and below [ ] 18 -24 [ ] 25 – 34 [ ] 35 – 44 [ ] 45 – 54 [ ] 55 – 64 [ ] 65 years and above [ ]

3. What is your role in the organization?

   IT Manager [ ] Security Specialist[ ] System Administrator [ ]System Analyst [ ] Database Administrator [ ]

4. How long have you been working in the IT industry?

1-3 years [ ] 4-6 years[ ] 7-10 years[ ] 11-13 years[ ] 14-16 years[ ] 17-20years[ ] 21 Years and above

5. How long has your organization been using cloud computing service?

   Less than year [ ] 1-3 years [ ] 4-6 years 7-10 years [ ] 11-13 years[ ] 14-16 years[ ] 17 years and above

PART 2: COMPLIANCE WITH INDURSTRY STANDARDS

6. Our organization complies with relevant industry standards for cloud security Strongly Agree [ ] Agree [ ] Neutral [ ] Disagree [ ] Strongly Disagree [ ]
7. Ensuring compliance with industry standards in our cloud environment is challenging Strongly Agree [ ] Agree [ ] Neutral [ ] Disagree [ ] Strongly Disagree [ ]
8. We have faced penalties or fines for non-compliance with industry standards in the cloud. Strongly Agree [ ] Agree [ ] Neutral [ ] Disagree [ ] Strongly Disagree [ ]
9. Regular audits help us maintain compliance with industry standards in our cloud environment. Strongly Agree [ ] Agree [ ] Neutral [ ] Disagree [ ] Strongly Disagree [ ]
10. Compliance training for employees is effective in ensuring adherence to industry standards Strongly Agree [ ] Agree [ ] Neutral [ ] Disagree [ ] Strongly Disagree [ ]

PART3: INSIDER THREATS

11. Our organization is highly concerned about insider threats in our cloud environment. standards

    Strongly Agree [ ] Agree [ ] Neutral [ ] Disagree [ ] Strongly Disagree [ ]

12. We have experienced insider threat incidents related to cloud computing in the past year

    Strongly Agree [ ] Agree [ ] Neutral [ ] Disagree [ ] Strongly Disagree [ ]

13. Our current measures are effective in mitigating insider threats in our cloud environment

    Strongly Agree [ ] Agree [ ] Neutral [ ] Disagree [ ] Strongly Disagree [ ]

14. We regularly monitor and log activities to detect potential insider threats

    Strongly Agree [ ] Agree [ ] Neutral [ ] Disagree [ ] Strongly Disagree [ ]

15. Access control in our cloud environment are sufficient to prevent unauthorized access by our insiders.

    Strongly Agree [ ] Agree [ ] Neutral [ ] Disagree [ ] Strongly Disagree [ ]

PART4: EMPLOYEE TRAINING SESSION

16. Our organization provides regular training on cloud security to employees.

    Strongly Agree [ ] Agree [ ] Neutral [ ] Disagree [ ] Strongly Disagree [ ]

17. The cloud security training we receive covers all necessary topics (e.g., data protection, access management, incident response).

    Strongly Agree [ ] Agree [ ] Neutral [ ] Disagree [ ] Strongly Disagree [ ]

18. The current cloud security training programs are effective in raising employee awareness.

    Strongly Agree [ ] Agree [ ] Neutral [ ] Disagree [ ] Strongly Disagree [ ]

19. Our organization conducts regular assessments to test employee awareness and response to security threats.

    Strongly Agree [ ] Agree [ ] Neutral [ ] Disagree [ ] Strongly Disagree [ ]

20. Employees frequently report security concerns or suspicious activities related to cloud computing. Strongly Agree [ ] Agree [ ] Neutral [ ] Disagree [ ] Strongly Disagree [ ]

21. Our organization is proactive in updating training materials to address new cloud security threats. Strongly Agree [ ] Agree [ ] Neutral [ ] Disagree [ ] Strongly Disagree [ ]

22. There is an impact of various security challenges in cloud computing, such as data breaches, insider threats, and insecure APIs, on the overall security posture of organizations that are implementing cloud services.

    Strongly Agree [ ] Agree [ ] Neutral [ ] Disagree [ ] Strongly Disagree [ ]

APPENDIX II: RESEARCH BUDGET

Table 16:Research Budget

ITEM	COST
Printing	2000
Transport	6000
Food	7000
Miscellaneous	5000
Total	20000

Table 17: Research budget

APPENDIX III: WORK PLAN

Table 18:Work Plan

TIME ACTIVITY	**SEPTEMBER**	**OCTOBER**	**NOVEMBER**	**JUNE**	**JULY**
Correcting presented proposal					
Preparing questionnaires					
Data collection					

Data analysis					
Report writing and submission					