THE UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING AND INFORMATICS

THE IMPACT OF ORGANIZATIONAL CULTURE ON INFORMATION SECURITY COMPLIANCE CULTURE: A CASE OF KENYAN UNIVERSITIES

Erick Ochieng Otieno

Supervisors:

Dr. Andrew Mwaura Kahonge

Prof. Agnes Nduku Wausi

A Thesis Presented for the Award of Degree of Doctor of Philosophy in Information Systems School of Computing and Informatics University of Nairobi, Kenya
2021

DECLARATION

I hereby declare that this project is my work and has, to the best of my knowledge, not been submitted to any other institution of higher learning.

Student: Erick Ochieng Otieno Registration Number: (P80/51691/2017)

Signature: .... Date: 17/November/2021

This thesis has been submitted for examination with my/our approval/knowledge as university supervisor(s) Supervisors

Supervisor: Dr. Andrew Mwaura Kahonge

Signature: .... Date: 18-November-2021

Supervisor: Prof. Agnes Nduku Wausi

Signature: .... Date: 18/11/2021

DEDICATION

To my late mother, *Rose A. Otieno*, who could not be around in person to celebrate with me this noble milestone. The confidence you had in me has made me who I am 24 years since you departed.

To my loving wife, *Syprose A. Ochieng*, who has seen me through the difficult journey. The understanding and the time you took to support me, and the family enabled me to focus more on this journey.

To my little boy, *Evan L. K'Ochieng*, who joined us in the middle of this journey, I dedicate this work to you to inspire you and be a reminder that with dedication and discipline you can achieve all you want.

ACKNOWLEDGEMENTS

I take this opportunity to thank both my supervisors who did their best to help me navigate this journey with their valuable advice and critiques. The time you took and the energy and dedication with which you supported me in refining this work were very appreciated. I also want to acknowledge the immense contribution from the respondents and others who supported in building up my knowledge in depth and in breadth towards completing this thesis. I want to specifically thank my spouse who read through the draft thesis reports to help me streamline the thesis. To the close family and friends who encouraged me, during the challenging moments, I thank you. Lastly, thanks to all those who played a role in different ways to give advice, critique, and help in the process of developing and completing this thesis.

ABSTRACT

Insider threat to information security is increasingly becoming a challenge to information security managers. One of the biggest challenges is not a lack of strong and robust policies, but that of ensuring full or highest rate of compliance with the policies. This is more compounded by the threats posed by insiders who have unfettered access to information systems assets. It is no surprise then that despite heavy investments in ensuring information security infrastructure, institutions still face the highest rates of information security breaches. Numerous studies have been conducted to provide insights and models on information security mitigations. However, very few studies have considered the policy compliance culture phenomenon. Among those who have considered the mixed methodology approach, none of the scholarly studies have considered grounded theory methods. The overall objective was to establish the relationship existing between organizational culture and information security compliance culture. As part of the Specific objective, the study intended to; 1) explore the relationship that exists between organizational culture and the actual information security compliance culture in universities in Kenya, 2) explain the relationship that exists between organizational culture and the actual information security compliance culture in universities in Kenya through theory generation, 3) and validate the theoretical model that predicts information security compliance culture.

The study employed an exploratory sequential mixed-method research design. This followed the QUAL-Quan principles. The population of this study was the Universities in Kenya. The study was divided into two phases namely, the model development phase and the model validation phase. The model development phase was designed to achieve two objectives namely: exploring the factors that impact information security compliance culture and explaining the relationships between the emerging factors and information security compliance culture through theory generation. The model validation phase was designed to test and validate the emergent theory through a semi-structured questionnaire. The model development phase adopted a grounded theory methodology while the model validation phase adopted the survey questionnaire approach.

The resulting theory was analysed and discussed in terms of model development and model validation. In the model development phase, several themes emerged which upon consolidation, were grouped into 4 main thematic groupings namely, demographic-oriented themes, organizational-oriented themes, individual-oriented themes, and information security compliance culture-oriented themes. The organizational oriented themes were further sub-grouped into the organizational level factors and moderating factors. The same was also done for individual-oriented themes to generate the individual-level factors and the factors moderating the individual-level factors. The study thereafter generated a theoretical model that explained a relationship between organizational initiatives, independent behavioral trends, management support, individual demographic interventions, and external organizational interventions towards information security compliance culture (ISCC). The model validation phase produced findings that supported the emergent theoretical model by having factor loadings that significantly supported the model among other parameters that were tested.

The study makes a main theoretical model contribution which is highlighted based on the model developed in phase one and the validated theoretical model. The model is adaptable to future researchers interested in covering information security compliance studies. The other contribution that this study makes is the methodological contribution which is also discussed in line with the efficiency of the procedures this study efficiently adopted. Further, the application of mixed methods as adopted in this study will provide insights to future information systems researchers to consider when deciding on how to conduct behavioral related studies. In terms of practice, the emergent theoretical model will be beneficial to practitioners in formulating checklists geared towards strengthening information security compliance regimes within their policy directions. This study is important because it provides a theoretical direction and methodological directions for future exploration of information security-related studies.

Keywords: Insider Threats, Information Security, Compliance Culture, Mixed Methods, Grounded Theory

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

CERT	– Computer Emergency Response Team
CFA	– Confirmatory factor Analysis
CIA	– Confidentiality, Integrity, Availability
CVF	– Competing Value Framework
DT	– Deterrent Theory
ERP	– Enterprise Resource Planning
GDT	– General Deterrent Theory
GT	– Grounded Theory
ICT	– Information and Communications Technology
IDS	– Intrusion Detection Systems
INFOSEC	– Information Security
IP	– Intellectual Property
IPS	– Intrusion Prevention System
IS	– Information Security
ISO	– International Organization for Standardization
ISP	– Information Security Policy
ISCC	– Information Security Compliance Culture
IT	– Information Technology
NIT	– Neo-Institutional Theory
PMT	– Protection Motivation Theory
QR	– Qualitative Research
SBT	– Social Bond Theory
SLT	– Social Learning Theory
TOE	– Technology, Organization, and Environment
TPB	– Theory of Planned Behavior
TRA	– Theory of Reasoned Action

1.0 INTRODUCTION

1.1 Background of Study

Prior researchers have asserted that a significant challenge for organizations is the task of encouraging employees to comply with information security policies and culture (Greene, Gwen & D'Arcy, 2010). Failure to comply with information security policies makes organizations vulnerable to insider threats (Bishop & Gates, 2008). The assumption has been that the risk and likelihood of a threat from within were low in comparison to external threats (Hong et al., 2010). While outsider threats are more prevalent, insider threats are regarded as wore costly and detrimental to organizations (Gheyas & Abdallah, 2016). In 2010, a US Army soldier released a large set of classified documents to WikiLeaks; and in 2013, a former contractor of the US National Security Agency disclosed thousands of classified documents to several media outlets. These incidents shook organizations to the core, forcing them to re-evaluate the trust that can be placed on internal employees. Organizations have a good reason to be worried because the incidents mentioned above are not isolated cases of insider attacks and non- compliance to security policies (Thing et al., 2017). Recent studies have established that the weak or lack of information security compliance culture in an organization is a major vulnerability that employees exploit to launch insider attacks (Kolkowska et al., 2017).

Insiders may be considered as the employees or individuals having access privileges, and vast vital knowledge of internal organizational assets and processes. These privileges and knowledge may be a critical precursor to the exploitation of weaknesses emanating from the organizational information systems. This exploitation may occur consciously or unconsciously (Willison & Warkentin, 2013). Insider threat outcomes can be classified into four broad categories namely: *sabotage*, *fraud*, *intellectual property theft* (IP), and *espionage* (Moore, et al., 2011). Many organizations and institutions have at one point in time been faced with one or many attacks emerging from these broad categories. For example, according to Kigen, et al., (2014) the year 2013 saw Kenyan organizations experiencing insider threats as the major security incidents. These incidences of malicious activities were deliberately instigated by current employees (Kigen, et al., 2014).

A recent report indicated that a mobile company was forced to incur 25 million US Dollars due to an insider breach. This was after the employees of a call center in Mexico, the Philippines, and Colombia accessed personally identifiable data of about 278000 customer account (Chabrow, 2015). The breach took place at a giant mobile telephone company's call center.

In the financial industry, despite the high-level information systems security investment, cases of laxity in security practices have been reported. These laxities have led to bad employees using the accumulated privileges or knowledge to subvert existing safeguards. Such cases of privilege abuse have occasionally been resolved by ensuring segregation of duties at a policy level (Technology Engineering Group, 2014).

A report by Verizon Enterprise Solutions, (2015), indicated that top breach incidents (55% of incidents) were privilege abuse. These occurred by the perpetrators taking advantage of one's legitimate access to commit illegal acts either for personal or financial gain. According to the 2014 United States' state of cybercrime survey (CSO Magazine, USSS, CERT & PWC, 2014), damages incurred due to insider attacks were found to be more damaging than outsider attacks. These incidents included but not limited to private or sensitive information unintentionally exposed which was estimated to be (82%), confidential records compromised or stolen which accounted for (76%), customer records compromised or stolen which was attributed to (71%), and employee records compromised or stolen was estimated to account for (63%).

Universities all over the world are faced with similar challenges of ensuring that information within their jurisdiction is held confidentially, has the integrity to the highest degree, and is always available when needed. Due to the tricky balance that universities must contend with regarding giving access to students, staff, and external stakeholders, issues such as how to ensure robust information security compliance emerge.

Many University institutions have already invested heavily to protect their systems from external intrusion and invasion using firewalls, controls, and processes among other security measures (Irwin, 2020). This means that it would take a lot of effort by external aggressors to penetrate and pose a risk to the intuitions' information or data within their systems.

Despite the safeguards in place, many of these universities still fall victim to attack from either those who are still employees or past employees. Some universities have also fell victims to breach emerging from students and stakeholder intrusions. This has forced many institutions to find unconventional ways of addressing the challenges. For example, a study by Alshare, et al., (2018) revealed that procedural and distributive justice, as well as an organizational culture among others, significantly predicted how severe information security violations were in an organization. The challenge is usually how to deal with those who are authorized to access the information due to their primary role, or secondary role, or proxy roles. In Kenya, a study by Sirma, et al., (2014) revealed that there still existed week relationship that was exhibited between the information security policies put in place and the net security breaches. That the security policies had no impact on the reduction of information security breaches implies the need for paradigm shift fronted by this study. It is our submission, therefore, that the extent to which information security is achieved depends on policy compliance by all who interact with the various information system assets. It can therefore be argued that compliance with information security policies thus becomes a very important factor for the information security managers in these institutions.

It has been established that data breaches everywhere in most cases end up being very costly for the affected organizations. In universities across the world, this is no exceptions. Several universities have appeared in the limelight for breach of data across the United States such as the University of Maryland, George Mason University, Butler University, and the University of Wisconsin-Parkside. Reports indicated that in 2014 alone, the University of Maryland experienced a data breach in which close to 288,000 data relating to students, and faculty members were exposed in a computer attack (Roman, 2015).

Besides, technology has also advanced in terms of sophistication and accessibility of information systems to many users from all social-economic spectrums. With this advancement, organizations find it useful to employ the usage of information system tools at all levels. This has led to increased risks emerging from liberalization, and deployment of these information systems (Maarop, et al., 2015). Safeguarding data is one of the greatest worry universities have because of the confidentiality, integrity, and availability-related aspect as already highlighted. Therefore, ensuring that student data, staff data, stakeholder data, and other critical information about research are safe is paramount.

It has always been traditionally considered that technological controls together with processes are a default approach to handling matters related to information security, however, this has since changed (Werlinger, et al., 2009). As such, in addition to technological processes and controls such as administrative, many organizations have invested heavily in, legal, physical, preventive, detective, and corrective controls to ensure information security. Despite all the actions, many still struggle to minimize the threats coming from within as aptly implied by (Colwill, 2010). Colwill, (2010) cautions that managing insider threats by overreliance on technology without considering other factors such as social, business, and cultural components can lead to disastrous results.

1.1.1 Organizational Culture

From a society's point of view, culture plays a big role in shaping the respective members' perception of the definition of what is right or what is wrong. Organizations are also no different since the key component of the organization is the employees or other stakeholders who may also form part of a given society. As such, the behaviours of each employee are different in terms of how they interact with the designed systems within the organizations.

The origin of the term organizational cultures is unknown, but the notion that factories, schools, and other institutions have cultures has existed for at least a half-century (Jaques, 1951). In the 1960s, it was not unusual to describe culture as the best way to get a handle on organizational development (Eisenberg & Riley, 2001). In the latter part of the 20th century, numerous scholars became entranced with the idea that understanding companies, churches,
universities, government agencies, student clubs, or indeed any form of institution or organization could be enhanced through a cultural analysis or critique (Eisenberg & Riley, 2001). The speed with which "organizational culture" emerged as a significant lens for scholars and other academics to examine or otherwise engage with organizations and institutions was astounding (Eisenberg & Riley, 2001). This lens is now entrenched in examining information security in organizations established by researchers in information security, including (Kolkowska et a1., 2017; Teoh & Mahmood, 2017; Otieno, Wausi &, Kahonge 2020). The problem of weak or lack of information security compliance culture in an organization has been attributed to the ever-increasing challenge of an insider attack by employees. The manifestations of insider attack imply that employees do not always comply with the set policies or organizational culture expectations.

Organizational Culture has variously been defined by many scholars in different ways for many years. Every author has had to put into context what was behind the definition to enable proper understanding for other scholars who have an interest in understanding organizational culture as a phenomenon.

Terrence Deal and Allan Kennedy gave a simple definition and summarized organizational culture as a way the respective group does things around where they are, or where their group of persons converges in day to day interactions (Deal & Kennedy, 1982).

Geert Hofstede, on the other hand, approached the definition from a mindset point of view. Hofstede, (1993) defined organizational culture as a collection of distinguishing programming that occurs in the mind, thereby giving distinct characteristics of different groupings of people or that which elicits different categorization of people from each other (Hofstede, 1993)

Gareth Morgan, for example, fronted a definition that implies that Organization Culture can be defined as the phenomenon in which the respective people actively live with results in a jointly created environment, and environments that the respective group of people lives in (Morgan, 1997)

Edgar Schein on the other hand defined organizational culture to be a consistent pattern that members of a group exhibit within systematic shared basic assumptions. These assumptions, according to Edgar Schein are acquired from numerous incidents of learning as the group continued solving the various external adoption as well as internal integration. In most cases, these solutions have yielded positive results in the past to warrant acceptance and thereby giving compelling reasons for every new member to be introduced as a norm, and the acceptable way to conduct themselves, and interact with the respective problems (Schein, 2004).

In addition to the various definition of what culture is by various authors, all the authors agree that organizational culture must also exhibit four extra elements to be considered as such. These elements in consideration are structural stability element, cultural depth element, cultural breath element, and aspects of patterns of the cultural manifestation or the integration therein.

Organizational culture can be said to have three major levels as espoused by Edgar Schein. Schein, (2004) indicates the three levels to include, artifacts, espoused beliefs, and values as well as the underlying assumptions (Corriss, 2010; Schein, 2004). In addition to the levels of organizational culture, one more important concept applicable to this study is the organizational subcultures. This is because an organization is not a monolithic environment, but is made up of various individuals with different characteristics such as, job descriptions, level of staff roles, educational background, professional background, and many others that define some of the groupings within it.

Artifacts

Artifacts are perceived to be those organizational structures that manifest themselves and organizational processes that are visible to anyone studying organizational culture, and are considered hard to interpret while observation of the level remains rather easy (Schein, 2004; Bibikas & Kargioti, 2010). Through their research findings Homburg & Pflesser, (2000) further supported the role artifacts play in the determination of behaviours emanating in organizations.

According to (Schraeder, et al., 2005) the Artefacts can be said to include the respective ceremonies, and numerous rituals organizations hold to their employees, the organizational symbols that organizations hold as important to them, together with the slogans that come with the symbols, and the narratives that are shared based on the respective events that have impacted the organization's success or failures passed to the new and old employees.

Espoused Values

Espoused values have been explained as the respective group strategies, group goals, and group philosophies that emerge after what the respective group can consider as justifications for their actions in the course of their interactions (Schein, 2004). Espoused value as an attribute of organizational culture has been argued to support instances of organizational artifacts as highlighted by (Nahm, et al., 2004). In other words, espoused values are considered as the various beliefs that manifest themselves in an organization grouping (Nahm, et al., 2004; Cooke & Szumal, 2000). It is argued that managers in organizational setup are the most vital sources of espoused values that are adopted in a cascading manner through the entire organizational fabric (Crane & Harris, 2002).

Underlying Organizational Assumptions

The last culture level, according to Schein, is the *underlying assumptions* that Schein, (2004) defines as the elements of an organization. The underlying assumption is considered as the definitive source in which values of the organization and actions of the organization emerge. The underlying assumption is also considered to be characterized by the beliefs that are normally taken for granted, or psyche, or the varied views, varied notions, and emotions (Schein, 2004). There is a school of thought among scholars who posit that the essential Underlying Assumptions form the fundamental foundations of organizational values and actions as well as acting as a tool to assist in ascertaining the import of artifacts and espoused values by deciphering any underlying assumptions that may exist within organizations (Nahm, et al., 2004).

The fact that organizational culture drives many facets of organizational practices and operations is not in doubt. This is evident in the works of many authors who have studied the relationships of organizational culture existing in many forms (Uddin, et al., 2013; Gregory, et al., 2009; Khazanchi, et al., 2007; Nahm, et al., 2004). Further, Sinclair, (1993) posited that organizational culture had some influence on how people in an organization behaved in terms of their ethical leanings. The authors also indicated management had an opportunity to apply organizational culture to resolve any issues that arose to improve organizational performance.

Organizational Subculture

Every organization exhibits a form of cascading or distinct subcultures under the greater Organizational Culture. The origins could be traced from organization's demography, social groupings, professional groupings, administrative groupings, customer-oriented grouping among many other multifaceted groupings, or categories of staff within an organization (Hofstede, 1993; Denison & Mishra, 1995; Hofstede, 1998; Schein, 2004).

The existence of subcultures in organizations manifests in scholarly works that have shown subculture existing in organizations in the form of subgroupings as shown by (Sackmann, 1992). Hofstede, (1998) avers that one can identify three dissimilar subcultural groupings as the professional grouping of a subculture, the administrative grouping of a subculture, and the customer-oriented grouping of subcultures. This makes this study also consider the possibility of having the Information Security subculture as a phenomenon of the organization considering the different subgroupings that may exist such as IT experts, administrative, and many others.

1.1.2 Information Security Culture

There seem to exist linkages in which organizational culture influences Information Technology and the other way around (Knorst, et al., 2011). This results in the formation of behavioral groupings emanating from influences of technology diffusion and social grouping setup.

Scholarly works by Gregory, (1983) and Smircich, (1983) support the argument of the existence of subcultures by confirming that relatively, organizations considered to be large tend to create subcultures as opposed to smaller ones which tend to have a homogeneous culture. Subculture has been found to play a very important role in creating what is considered as strong culture organizations (Schein, 1993; Boisnier, 2002).

Other studies that have also investigated the area of information security culture was that of Tang, et al., (2015) which addressed their research towards information security culture concerning organizational culture. Their study considered constructs that were used to generate interview designs for their respondents.

This study considers information security culture as an integral part of the greater organizational culture that can be considered a subculture that needs to be studied. This position is also supported by Schlienger and Teufel who considered the information security culture as subcultures in organizations (Schlienger & Teufel, 2003). The authors argued that the subculture encompassed all mitigations related to organizational socio-culture that supported technical security actions, aimed at making every organizational staff naturally embrace information security as a day to day norm (Schlienger & Teufel, 2003).

But what is the information security culture? The answer to this question can be summarized by the work of Alhogail and Mirza, who argued that Information Security culture can be described as a totality of guiding principles of how humans interact with information assets within an organization. These guiding principles influence the behavior of employees with regards to the preservation of information security in which the perception, values, attitudes, assumptions, and knowledge becomes the foundation (AlHogail & Mirza, 2015)

In their work, Alhogail and Mirza proposed a new framework that incorporated managing of change aspects that could offer guidance in cultivating information security culture, and which emphasized four pillars namely, responsibility pillar, preparedness pillar, management pillar, and regulation pillar (AlHogail & Mirza, 2015). Information security culture acts as a guiding pillar of how things are carried out within organizations about information security. The sole objective of the pillars is information assets protection as well as influencing employees' security interactions (AlHogail & Mirza, 2014).

1.1.3 Adopted perspective to organization culture

Based on the above, this study adopted the concept of organizational culture to imply a group of visible and invisible cues that emerge from values, norms, assumptions, institutional artifacts that organizations pass on from one generation of members to the next. These cues create the guiding pilar that shapes the behavior, aspirations, and conscience of any organization. We also adopt the concept of a subculture within organizations that may be shaped by existing organizational culture practices.

1.1.4 Information security compliance culture

We consider the trend already set by previous authors of organizational culture concerning information systems such as (Schein, 1993; Boisnier, 2002; Schlienger & Teufel, 2003; Tang, et al., 2015). As such, we propose the existence of an information security compliance culture. As argued by many researchers about the embedding of information security culture in organizations, we add to this call by narrowing it down to policy compliance culture. Understanding the impact of organizational culture on information security compliance culture was what this study undertook.

1.1.5 Approaches to Studying Organizational Culture

Understanding how to build and develop a concept of organizational culture needs clear guidance on how to work with its definition, its measurement, its study, and its application to organizational setup as its real world. As such, it would be appropriate to look at which study approach would befit the aspect of study and define Organizational Culture.

Several approaches to studying organizational culture have been proposed by Edgar Schein. These could entail the Survey Research approach, Analytical Descriptive approach, Ethnographic approach, Historical approach, and Clinical Descriptive approach (Schein, 1990; Schein, 2004). Schein further adds that the approach a researcher takes would be dependent on how the organization under study is engaged with the researcher and how the respective organization members become engaged in the process of data collection (Schein, 2004).

Compliance with IS Policies

It could be argued that without a strong compliance strategy with information security policy and regulations, many organizations will still be having a big problem in tackling the insider threat problems. A study by (Siponen, et al., 2010) revealed that failure by employees to comply with the organization's policies and procedures posed a major threat to information security.

Many non-compliance incidents are because most employees are not aware of the laid down policies and procedures. As indicated by Bulgurcu, et al., (2010), information security awareness played a very important role in employees' compliance. The same thought had also in earlier literary work been alluded to by Siponen, (2000) in which the author argued that a persuasion strategy would enhance awareness which would, in turn, minimize the errors occurring when employees do not comply due to ignorance.

Despite there being available many controls and processes such as administrative, logical, physical, preventive, detective, and corrective controls that guide the mitigation of insider threat, there remains a bigger and more potentially damaging threat to organizations from those insiders who have access to the internal systems. This is because even though the said organization may have very robust policies and controls and processes, the employees may not be so enthusiastic as to comply with the same robust policies and controls and processes.

Several strategies and approaches have been availed by different players to ensure that employees or stakeholders comply with the laid down policies. Some compliance strategy emphasizes behavioral and managerial artifacts such as applying threat tools and reward tools to help shape the attitudes towards complying with policies in organizations (Siponen, et al., 2010).

Neutralization of the information security violations before they occur has been fronted as one of the other strategies, apart from threat and reward approaches, to promote information security compliance in organizations, especially where employee’s intentions to violate information security are monitored and thereby discouraging non-compliance (Siponen & Vance, 2010).

1.1.6 Theoretical and Knowledge Gap Assessment

There is overwhelming extant work that has covered information society compliance or information security culture. However, there is very minimal attention towards factors that contribute or antecedents that can explain information security compliance culture. This is even expounded by the fact that the articles that have attempted to address the aspect of information security compliance culture have failed to let the antecedents evolve naturally in their setting. Theoretical discovery is key to developing a theory in an area that is minimally covered such as information security compliance culture. A look at a few articles that have dwelt on information security as an area of inquiry can be seen in such works from, Pahnila, et al., (2007), Herath & Rao, (2009), and Bulgurcu, et al., (2010) who applied theory of planned behavior to address the issue of awareness in shaping information security behavior. This however failed to address the aspect of information security compliance. We further look at the study by Kankanhalli, et al., (2003) which adopted the organizational culture theory to investigate how the fear of sanction shaped decisions of non-compliance with information security policies. In all these studies, none addressed the other possible antecedents within a given context such as our study that adopted grounded theory and let the variables emerge on their own without predicating them on existing theoretical constructs.

We can therefore say that despite the overwhelming theoretical maturity around information security and by extension information security compliance, the same cannot be said to be true around information security compliance culture. Therefore, we argue that this constitutes a lacuna in theoretical underpinnings in the study of information security compliance culture. This leads us to assess the knowledge gap that this study will also attempt to contribute to. As seen in Table 1, several works are assessed to identify the researchers(‘s) study focus, the key findings, the knowledge gap, and how this research handled them in the study.

Table 1: A summary of the theoretical gap and Knowledge Gap Assessment

Researcher(s)/ Author(s)	Study Focus	Finding(s)	Knowledge/theoretical Gap	How it will be handled in the research
Ifinedo, (2014)	The study applied an empirical approach that considered socialization, influence, and cognition. This was studied through the "*Deterrence theory*" lenses.	Key findings showed social bonds formed at work influenced attitudes towards compliance and subjective norms. The two constructs also emerged as having positive effects on ISSP compliance efforts by employees.	The study, however, fell short to address the components of compliance culture which this study argues to be key towards long-term ISSP compliance. The utilization of existing theory to draw antecedent also did not give room to other equally important constructs to be considered.	Our study therefore will adopt the grounded theory approach to let the free discovery of new constructs to build its theoretical antecedents that can explain the compliance culture elements that are lacking in this study
Safa, et al., (2016)	This study applied hypothesis testing to generate a model for information security compliance in organizations. Through the application of the "*Social Bond Theory*", the study proceeded to investigate the roles played by aspects of involvement as prescribed by the "*Social Bond Theory*".	Key findings showed that Involving members of the organization positively influenced how they complied with information security policy. The study also identified that commitment by members leads to a positive influence on information security policy compliance. Further, the study findings showed that there was a positive influence on information security policy compliance through personal norms positively.	The study, however, failed to delve deeper into how these constructs relate to information security compliance culture. The limitation of the singular application of one theoretical perspective also meant that there could still be more antecedents out there that could give more explanations towards information security compliance culture	It is from this premise that this study sought to investigate these antecedents as discovered through the grounded theory model development phase.
AlKalbani, et al., (2017)	The authors approached their study from the hypothesis testing point of view to look at the role institutional pressure plays on information security policy compliance.	The findings show that information security compliance motivated the management to increase their commitment towards effort for information security compliance.	The study made great contributions towards relating institutional pressure to information security compliance. However, the approach of using singular antecedent to test left other potential constructs that could not be identified due to the prior approach.	This study opted to handle this gap by adopting a methodological approach geared towards the discovery of antecedents and theoretical development that will form a basis of information security compliance culture study

Researcher(s)/ Author(s)	Study Focus	Finding(s)	Knowledge/theoretical Gap	How it will be handled in the research
			The study also did not consider the cultural aspect of compliance with information security policies.	
Amankwa, et al., (2018)	The authors factored in variables from the involvement theory and organizational behavior theory to develop their hypothesis	The study found that factors such as supportive organizational culture and end-user involvement significantly influenced employees' attitudes towards compliance with ISP. The overall results showed that employees' attitudes and behavioral intentions towards ISP compliance together influenced the establishment of ISCC for IS compliance in organizations.	The study fell short of going deeper to in identification of components of information security compliance culture. This was attributed to the use of extant theories rather than exploring and generating new theoretical perspectives.	This study shall explore the respective elements of information security compliance culture as a sub-culture within the organizational culture. The Grounded Theory approach will enable the discovery of newer and more in-depth variables that can explain ISCC for IS compliance in organizations
Sommestad, et al., (2019),	The authors considered variables emerging from meta-analysis information security behavior tests. The meta-analysis based its antecedents on the "Theory of Planned Behaviour".	The key findings showed how the individual's anticipated regret and individual's habit improved the predictions on information security behavior.	The study, however, overlooked other aspects of information security behavior whether as predictors or as net effect and how these elements could lead to information security compliance culture	It is from this premise that this study sought to go beyond the approach and employ grounded theory in a bid to discover more elements, and thereafter explain the relationships via a theory generation.
Tang, et al., (2015)	This study addressed information security culture concerning organizational culture. The focus of the study was geared towards looking at how organizational culture	The study demonstrated how organizational culture impacts ISC. The study went ahead to shows the suitability of organizational culture theories such as Hofstede's	One major knowledge gap here is identified via their recommendations for future researchers to consider deployment of research in two directions possibly to validate the measure for ISC and to develop exploratory models for empirical tests targeting the impact of organizational culture on ISC.	This study, therefore, took the cue of the existential gap by choosing to conduct a mixed-method, one to generate dimensions grounded on data discovery and the second one meant to validate the emerging theoretical model from data discovery.

Researcher(s)/ Author(s)	Study Focus	Finding(s)	Knowledge/theoretical Gap	How it will be handled in the research
	impacted information security compliance. The study drew from Hofstede's organizational culture framework to generate the dimensions that were tested.	framework in offering explanations of the relationship between organizational culture and ISC.	Secondly, the acknowledgment of possible additional dimensions that could have been considered for their proposed ISC framework of this study exposed the antecedent's gap.	

1.2 Problem Statement

Prior studies have revealed that failure by employees to comply with the organization's policies and procedures posed a significant threat to information security (Greene, Gwen & D'Arcy, 2010; Siponen & Vanca, 2010). Despite the tremendous work on information security compliance by preceding researchers, the problem is still escalating and persistent (Sohrabi Safa et al., 2016; Greene, Gwen & D'Arcy, 2010). The current literature has asserted that insider threat is an information security problem (Ophoff et al., 2014). Moreover, IBM, (2019) reported that the per-record cost of a data breach for three root causes, the cost of data breaches due to insider threat malicious or criminal attacks was $166 per record. This is approximately 25 percent higher than the per-record cost for breaches caused by system glitches and human error, which were $132 and $133, respectively (CISA, 2019). In Kenya Sirma, et al., (2014) presents another existential challenge that indicates the disconnect between security policies and the quest to reduce information security breaches in Kenyan universities.

In terms of methodological and theoretical challenge, despite the existence of past work on controls and processes, most of the extant work has focused on either policy development approach, or systemic design to mitigate information security policy breaches. The existing information security compliance studies have looked very minimally at the role played by organizational culture in enhancing information security compliance (Ifinedo, 2014); Safa, et al., 2016; AlKalbani, et al., 2017). Those that have inquired about the area at length have taken a more quantitative approach and little qualitative approach. Little extant work has also focused on a different approach in their inquiry such as the grounded theory approach. For the few studies that have considered grounded theory as a method of analysis, little can be said about the application of the mixed method as a way of validating or truncating the emerging result

(Amankwa, et al., 2018). This study, therefore, sought to address these missing links by exploring the impact that may exist between organizational cultures on information security compliance. In the same latitude, this study sought to contribute to a methodological and analytical approach to the investigation of information security-related studies. The research took a unique tangent of considering mixed methods and adopting the grounded theory approach as the analysis strategy. The mixed-method approach aimed to provide the validation component of the emerging theoretical model from results grounded on empirical qualitative data. The eventual solution that this research contributed to is a theoretical contribution by way of a theoretical model that explains information security compliance.

1.3 Research Objectives

The overall objective was to establish the relationship existing between organizational culture and information security compliance. This study, therefore, considered a broader approach of behavioral, technology, and Organizational aspects concerning insider threats. The study sought to conduct empirical qualitative, and confirmatory quantitative study with regards to Information Security Compliance Culture (ISCC) as a way of mitigating insider threats.

Specific Objective:

- Explore the relationship that exists between organizational culture and the actual information security compliance in universities in Kenya
- Explain the relationship that exists between organizational culture and the actual information security compliance in universities in Kenya through theory generation
- Validate the theoretical model that predicts information security compliance culture

1.4 Research Questions

- What relationships exist between organizational culture and information security compliance in universities in Kenya?
- How do these relationships impact information security compliance culture in universities in Kenya?

1.5 Research Contribution

By building upon already available behavioral approach in mitigating insider threats, this study intended to increase contribution to the body of scholarly work by exploring a combination of several available models and availing a much stronger and more detailed approach to establishing compliance culture within organizations through employee behavioral, employee social and organizational environmental facets that influence the general compliance to insider threats to information system policies.

It is unclear for many students how to develop interview guides especially in cases where grounded theory is applied. It is equally unclear for many students how to effectively conduct grounded theory studies with the limited time and resources at their disposal and considering the principles of data saturation and rigor. Therefore, we contextualize our methodological contributions based on the flexibility that grounded theory (GT) exhibits (Birks, et al., 2013), which allows researchers to adopt the methodological framework while contributing to research. We approached our study by conducting literature to identify categories, then using the categories, we formulated interview guides. This assisted in identifying who to sample rather than casting the net wide. This, therefore, provided an opportunity to arrive at saturation faster, while still maintaining the core tenets of grounded theory. By adopting a procedural process of taking full advantage of the word document to do a line by line coding, the process enabled us to easily internalize the emerging construct and process the analysis very fast. Our methodological contributions can, therefore, be considered as a procedural contribution in the grounded theory process, and application of the mixed method to validate the results as part of the mixed method application in information security-related studies. A look through extant studies shows little focus on grounded theory as part of a mixed method. Our study therefore will give future students who would want to conduct mixed methods a chance to consider effective procedures while undertaking grounded theory either as part of a mixed-method or as a stand-alone approach. Our procedural approach also shows that it is possible to adopt manual coding processes as opposed to using sophisticated software in analyzing data that emerge from grounded theory. This approach has advantages in terms of bonding with the data and having ease in identifying categories and themes that emerge. Our contributions will inform future students while considering how large their data is or how small their data is to decide on whether to use software or to proceed and conduct manual data.

1.6 The Rationale of the Research

The study is important in that it contributes to developing a pool of information that can be used as consultative guidelines. The guidelines can be applied by policymakers dealing with insider security threats by introducing a model for information security culture in any enterprise.

We further get our major justification from a study by Wechuli, et al., (2014) in which after conducting a literature review on information security models, recommended further studies and research on best models that could offer the best solution.

Hunker & Probst, (2011), also gives a more compelling reason why such a study like this one forms a very vital part of the resource pool for insider threat mitigation scholarly work. In their recommendation for further work, Hunker & Probst, (2011) recommended a more refined redefinition as well as the categorization of various insider threats.

It is on these platforms that this study becomes highly necessary to try and contribute to the recommendations by the various authors and contributors to the area of insider threat mitigation strategies.

2.0 LITERATURE REVIEW

Theories have been suggested in scholarly works as a tool to inform the approach to be taken by the researchers. Dwivedi, (2009), theories are important to researchers due to their vital roles in the foundation base with which researchers can build their studies and organize their scientific inquiry. Theories help researchers generate constructs, analyze their findings, build their argument around a phenomenon, build their study, and many more (Gregor, 2006). A more synthesized and simplified value of theory in research is that fronted by Sutton & Staw, (1995) in which the authors aver that theories tell a story of why phenomena are said to be correlated as suggested by empirical analyses.

This study looked at various theories that explained the concept of organizational culture as well as compliance culture thereby creating an understanding and helping develop a theoretical model for this study. The theories that were investigated covered all social, organizational, and information system theories at large.

Since this study looked at relationships between organizational culture and information security compliance culture, it was prudent to understand the underlying phenomena by seeking to understand the organizational theory, Social theory, and information systems theory. To understand information security compliance concepts as a result of organizational culture, social pressure, and information security culture, it was ideal to look at the various behavioral theories such as the theory of reasoned action (TRA), the theory of planned behavior (TPB), general deterrence theory (GDT) and protection motivation theory.

2.1 Organizational Culture Theory

Organizational theory can be described as a process that organizations endeavour in the identification of configurations, and structures that can be employed in the processes of finding solutions to challenges faced to improve the efficiencies and productive obligations of an organization (Emirbayer & Johnson, 2008).

Before delving deeper into the organizational culture theory, it would be important to understand the various schools of thought with which researchers base their world view with regards to studies that involve organizations and culture therein. To this end, Gibson Burrell and Gareth Morgan argued that for an organizational research study, researchers need to take into consideration and think about which paradigms they are going to apply in the analysis of the organizations in the subject. Organizational studies field exhibit functionalist, interpretive radical humanist, and radical structuralist as the various basic paradigms as originally advanced by (Burrell & Morgan, 1979). Most of the available theories and models form the backbone on which organizational culture is hinged and fall within these world views. A case in point is Edgar Schein's model of Organizational culture which finds comfort in the functionalist paradigm (Schein, 1990).

2.1.1 Functionalist Paradigm

The functionalist school of thought is fronted as more positivist according to works by (Burrell & Morgan, 1979). The authors' arguments pointed to the fact that researchers planning to apply the functionalist approach mostly opted for hypothesis testing strategy. The aspect of reality and explanation of the context with which order is maintained by organizations and society at large is the pillar of the function's paradigm. The assessment approach through functionalist is more inclined towards the organizational functional components that the organization processes as a whole that constructs the organization (Safriadi, et al., 2016).

2.1.2 Interpretive Paradigm

The interpretive paradigm is said to be leaning heavily towards the explanation of how individuals subjectively experience, or perceive the environment around them in an organization, and is considered to be more inclined to help researchers understand processes within an organization, and the individual processes which influences the behavioral aspects in question (Smircich, 1983). The Interpretivist paradigm has been applied in studies by researchers to look in to form that a basic assumption takes in terms of meaningful interpretation, as well as how to interpret the organization's value system and its underlying philosophical basis employed to guide the interactions that exist between organization's members (Safriadi, et al., 2016).

2.1.3 Radical Humanist Paradigm

Just like the interpretivism paradigm, the radical humanist school of thought emphasizes the role played by an individual's subjective experiences in which any researcher as an external entity is obliged to engage and draw knowledge from the individual. However, the point of departure that exist between the radical humanist school of thought and interpretivism paradigm is evident from the fact that the main objective of the knowledge gathered in the radical humanist school of thought is to radically shift the social order from the existing one in an organization (Burrell & Morgan, 1979), and is mostly considered anti-organization. Therefore, researchers who consider the radical humanist school of thought lean towards not just interpreting the subjective views of the respondents but also to go further and change the way of thinking based on the resulting knowledge.

2.1.4 Radical Structuralist Paradigm

This paradigm forwards the school of thought that social situation causes the transformation of an organization (Burrell & Morgan, 1979). The organizational studies approach commits radical shifts and put more weight on the conflicts that arise from structures, domination modes, differences, and deprivation within the analysis and tends to be both positivist and realist in nature (Burrell & Morgan, 1979).

2.2 Organizational Culture Theories and Models

Understanding the dynamics of an organization calls for first and foremost, getting to understand the various theories and models that give light to the dynamics and baselines of how organizations operate. Theories and models are the best way to achieve this. Some several theories and models have been generated towards this end and a few have featured prominently among researchers studying the effect of organizations on performance, productivity, effectiveness among many other outputs of organizational interest. However, extant literature has little information on which theories can be pinpointed as the best one to adopt when studying and analysing organizational culture. Despite the challenge of a more robust and recommended organizational theory in the extant literature, there exist a few theories that have been applied numerously in organizational culture scholarly work such as competitive value framework. This study looked at a few of these models to have dimensions and constructs for its theoretical model with which it conducted the first phase of qualitative data collection.

2.2.1 Competing Values Framework

As one of the most widely applied models by many researchers across numerous organizational and management fields, the Competing Values Framework (CVF) found its way into the scholarly works through Quinn and Rohrbaugh. The model prides itself as one which specializes in organization analyses. Through this, researchers can apply specialization when looking into the organization's way of forging effectiveness, among other areas of interest such as organizational culture (Quinn & Rohrbaugh, 1983).

According to Cameron and others, CVF is a great asset to researchers and practitioners who are venturing into the characterization of individuals and leadership in organization as well as in the research touching on the organizational culture evaluation (Cameron, et al., 2007), due to its unravelled empirically-based evidence and the reality representation accurately (Cameron & Quinn, 2011). The model provides researchers with several dimensions of construct generations depending on the organizational construct through its four quadrants concept with each quadrant consisting of key significantly organizational and management theories.

In the field of information system research, CVF has been variously used to address several different areas of interest. For instance, a study by, Cooper & Quinn, (1993) applied the CVF to enhance the knowledge on how effective management information systems by seeking to understand the effectiveness constructs of management information systems under study.

One major observation that can be argued to be a setback to a researcher interested in analysing the entire organizational dimensions is that the Competing Values Framework can be considered as heavy on management dimension and light on employee dimensions making the resulting data possible of being one-sided. Organizations have multiple groups and subgroups interacting together to form common values, and this includes both management and non-management groups. Therefore, it would be more holistic to have a model that caters to all dimensions and generate constructs that can be attributed to all the entities of an organization.

2.2.2 Edgar Schein Model of Organization Culture

Schein theorized culture to exist in three levels namely; artifacts and symbols that are easily visible to anyone espoused values by the employees and the assumption that employees usually hold and need to be taken into consideration (Schein, 2004). These levels form part of past encounters and are emulated by a new employee who also tries to accustom to once they form part of the organizational family.

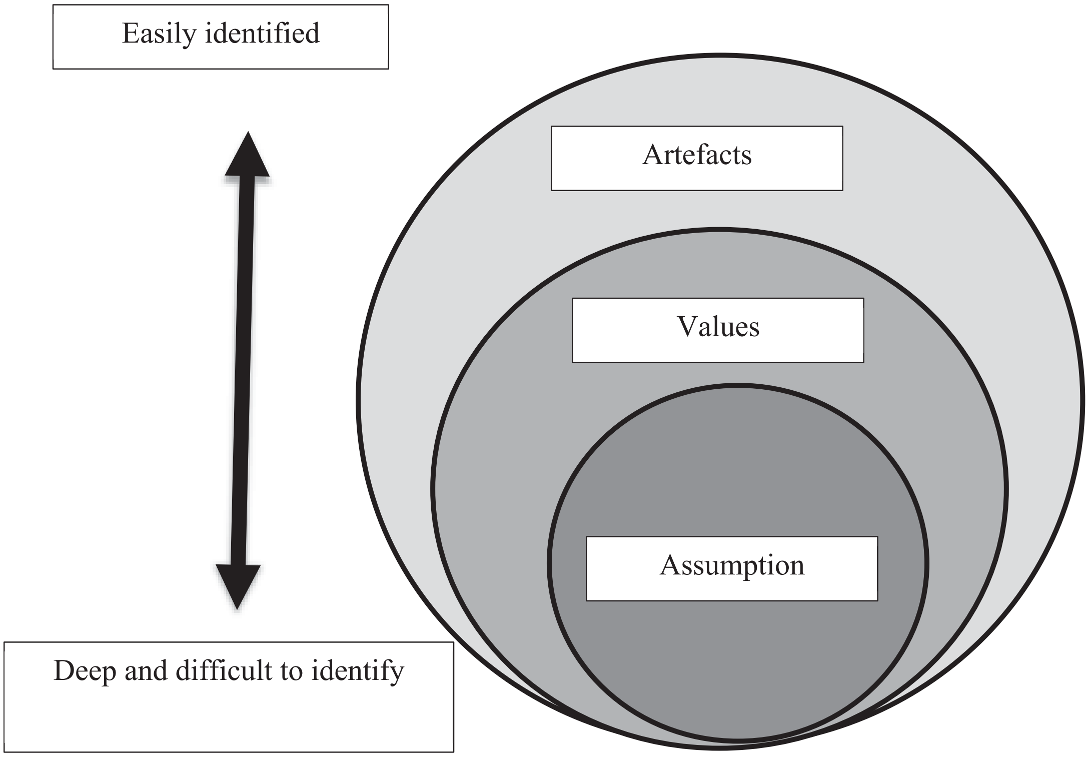


Figure 1: Edgar Schein organizational culture model

2.2.3 Hofstede Model of Organization Culture

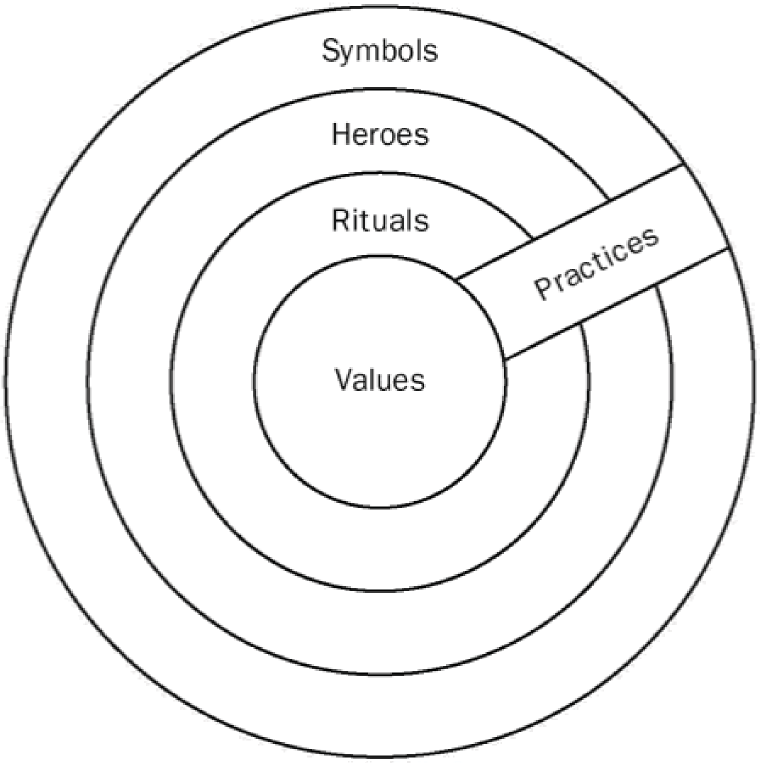


Figure 2: Hofstede organizational culture model (Hofstede, et al., 2010)

Approaching from a holistic approach of National and Organizational culture, Hofstede, et al., (2010) theorized the cultural concept from five dimensions which the author proposed as Power Distance, Uncertainty Avoidance, Individualistic nature vs Collective nature, Gender in terms of masculine attributes against feminist attributes, and long orientation attributes against short-term organizational orientation attributes (Hofstede, et al., 2010).

Despite the model receiving a few criticisms here and there such as the one from McSweeney challenging Hofstede's fundamental assumptions on the national cultures (McSweeney, 2002), and Ailon critically looking at some inconsistencies on the dimension values as proposed in Hofstede's (Ailon, 2008), the theoretical underpinnings are still considered as one of the most robust models for studying organization culture by scholars.

2.2.4 Johnson and Scholes' Cultural Web Model

One other model for the study and analysis of the organization is the model that was developed in 1992 by Johnson and Scholes known for its advocating for a holistic approach. The Cultural Web as the model is popularly known is argued to be the best tool for providing dimensions for researchers and practitioners who study and analyse organizations be it when seeking to understand the organization's culture, or when the practitioners want to change their organization's culture (Johnson, et al., 2008).

Unlike other models that have been proposed by other organizational culture authors, the culture model emphasizes the role of the assumptions that exist in the organization or the organizational paradigm as a basis for behavioral, physical, and symbolic organizational manifestations and vice versa. The cultural web can be used to understand the culture in any of the frames of reference discussed above but is most often used at the organizational and/or functional levels (Johnson, et al., 2008).

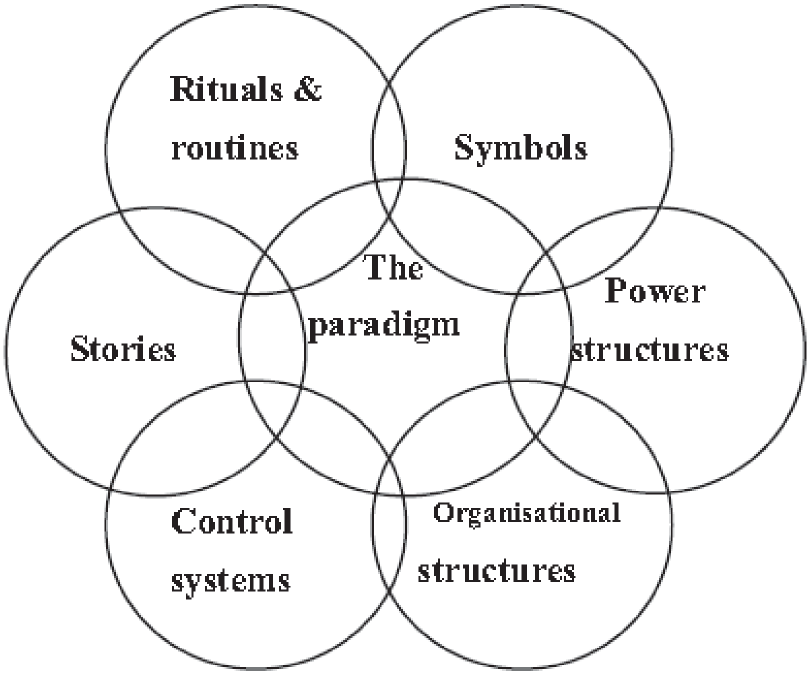


Figure 3: Johnson and Scholes' Cultural Web Model, (Johnson & Scholes, 1999)

As seen in Figure 3, the culture web model consists of seven components with the paradigm connecting all the other elements. The paradigm according to Johnson, Scholes, & Hallam forms the series of assumptions that an organization holds relatively as a common phenomenon and which most organizational members take for granted (Johnson, et al., 2008). The paradigm links other organizational elements such as routine and rituals, symbols, power structures, organizational structure, control systems, and stories.

2.2.5 Neo-Institutional Theory (NIT)

One other theory of interest to this study is the Neo-Institutional Theory (NIT) which was formulated by DiMaggio and Powell in the year 1983. The theory stipulated that stakeholders are deemed to be the foundation of organizational survival in that if the stakeholders lack confidence leading to failure of the organization to guarantee acceptability due to nonconformity with the respective stakeholder expectations, then organizations would be prone to failures (DiMaggio & Powell, 1983). DiMaggio & Powell, (1983), illustrates three main constructs can be synthesized from the Neo-Institutional Theory namely: coercive isomorphism, coercive isomorphism, and normative isomorphism.

Organizational perceptions have relatively emerged more as a cultural system as well as social systems as opposed to the traditional production systems (Scott, 2001). Institutional theory has grown since its inception to a concept applied in many facets of studies dealing with organizational issues such as organizational culture, and the growth can be attributed to works by (Meyer & Rowan, 1977; DiMaggio & Powell, 1983).

Institutions are made up of cultural-cognitive, normative, and regulative elements, which together with associated activities and resources offer stability and meaning to social life. Scott & Davis, (2008), indicates that the three forces are present in totally developed institutional systems, with economists and political scientists emphasizing regulative, sociological, and normative factors, and anthropologists and organizational theorists emphasizing cognitive-cultural factors.

It can be argued therefore that organizational behavior can be driven by the desire to look good and responsible in the eyes of the stakeholders. These behaviours with time create a necessity for deeply rooted aspirations that may or may not be passed through generations to generations of leadership and membership of the organization.

2.3 Application of Organizational Theories

Several authors have also applied a few or most of the elements found in the culture models found above to explain their findings while studying the impact of culture on their subject under study. One such case can be found in the study done by Ruppel & Harrington, (2001) among other factors such as ethical and developmental culture influenced how intranet was implemented in the organizations they studied, hierarchical culture also took a centre stage in facilitating the implementation. Looking at the culture web as depicted by Johnson & Scholes, (1999) it can be said that hierarchical culture falls under the element of the organizational structure of the model.

A study by Nahm, et al., (2004) also seems to adopt one of the organizational culture models by applying how Schein conceptualized culture and considering Schein's model of underlying assumptions, espoused values, and artifacts. This affirmed that indeed particular values and beliefs impact how managers behaved in an organization as well as higher performance resulting from espoused values. This shows that indeed Schein's model can be used by researchers to come up with a construct to that effect.

A study by Leidner & Kayworth, (2006) looked at the role played by cultural values in the study of impacts of culture at any level of analysis. They also seemed to advocate for the consideration of Hofstede's culture model by urging the consideration of organizational level values, and national level values at various stages of analysis. It can be remembered from Hofstede's model the emphasis placed on the national culture while studying organizational culture (Hofstede, et al., 2010).

Scholarly works such as that of Chang & Lin, (2007) on the other hand emphasized the values of an organization such as integrity, flexibility, etc., and explained how these values impacted information security management such as confidentiality.

A look at Jones, et al., (2004) works also shows that indeed if organizational members share beliefs, norms, and certain ideologies as a group, then this could lead to a firm's culture. The authors further noted the role organizational culture play within the context of organizational knowledge due to the important aspect of organizational members being able to create the organizational knowledge and acquire the same while sharing and managing the knowledge evolving from the organizational membership (Jones, et al., 2004) thereby creating a value and belief chain of symbols or artifacts for newer members to build their values and ethics on.

One other study that adopted the model of competing values framework as opposed to the other models was the study by Iivari & Huisman, (2007) in which their findings affirmed the role hierarchical culture played in the methodology deployed by information systems development. The authors argued that such hierarchical culture had a critical impact on the productivity of the groups adopting it as well as efficiency in ways of implementation and how goal achievements were met.

2.4 Information Systems Theory

In the information systems area of study, several theories have found their way as very useful to researcher due to the vital role they play in terms of their classification as explanation theories, prediction theories, both prediction and explanation theories, and lastly design and action theories which are all considered interrelated according to (Gregor, 2006).

Researchers studying information systems have benefitted a lot from theories borrowed from other disciplines such as studies dealing with economic issues, those studies covering psychology, studies evolving around computer science, and studies that considered general management (Wade & Hulland, 2004). Therefore, the information system is very rich with these theories applied to enhance the comprehension of the information system as an area of study.

There have been several attempts to highlight how several theories, in addition to models, have been employed in the study of information systems related research. Truex, et al., (2006) argues that there is a need to put into consideration the fitness between the theory that one has selected and the subject interest, historical context of the said theory, the impact the theory will have on the research method chosen, and the cumulative theory contribution that the theorizing will have on the outcome.

This study has considered several theories that are associated with information systems, and the linkages they have to the general employee’s interaction with information systems vis-a-vis information security policies within an organization. Information system theory that is related to organizational, environmental, as well as technological factors at the organizational level, is considered by this study as *Technology – Organization – Environment Model*.

2.4.1 Technology – Organization – Environment Model

Technology-Organization-Environment (TOE) is said to have been originally developed by DePietro, Wiarda & Fleischer. Construed as a theory applicable at an organizational level, the Technology-Organization-Environment (TOE) theoretical model has been a source of explanation. The theory refers to three elements that define a firm's contextual influence on how decisions affecting information systems are arrived at in an organization (Baker, 2012). Technology, organization, and environment are the basis from which three elements are derived from namely technological constructs, organizational constructs, and technological constructs (Baker, 2012).

TOE theory has been widely used in scholarly work by researchers interested in explaining the roles played by technology, organization, and environment within the context of information system interactions. Examples of these interactions include the adoption of Information Technology, the development of IT systems, rejection of IT systems, and many more. The organization element of the model has been applied by many researchers to identify constructs or factors to be considered for analysis on the relationships to adoption among others.

Even though TOE has been widely applied in the study of Technology adoption, there are many appearances of the TOE model in studies with information security compliance as a subject of study. Studies have shown that indicators of technological contexts and organizational contexts influence how people in an organization comply with information security compliance (AlKalbani, et al., 2015). Within the Organizational context, coercive institutional pressures, normative institutional pressures, and mimetic institutional pressures have been found to contribute to information security compliance (AlKalbani, et al., 2016).

TOE therefore can be considered as an asset to researchers interested in studying organizational antecedents such as management support, size, environmental influence on how decisions are made, and technological factors that make those interacting with the technology in an organization behave in a particular manner.

2.5 Social and Behavioral Theories

Social theories have been opined to conceptualize how human actions factor in the shaping of social systems (Coleman, 1986). In information system research, social theories have also been applied as seen in the studies by (Allen, et al., 2011; Shoib, et al., 2006). It is further argued by Shoib, et al., (2006) that social theories may be used in studies to generate a guide for ontology, epistemology, and methodology for the research. Additionally, social theories shape the researcher's chosen method. It also influences the structure and ingredient of the resulting functional theories and outcomes from research work.

Several other theories have been fronted as a basis of studies concerning human behavior. Available scholarly work has shown these theories that emerge from criminology and social behavior, being applied to study information security from human behavior perspectives. Mishra & Dhillon, (2006) argues that Deterrence Theory (DT), Theory of Reasoned Action (TRA), Social Bond Theory (SBT), Theory of Planned Behaviour (TPB), and Social Learning Theory (SLT) are some commonly applied theories in information security studies.

As indicated by Lebek, et al., (2013) amongst the theories appearing in the extant literature, the Reasoned Action theory (TRA) which has since been expanded to the Planned Behaviour theory (TPB) has been used the most standing at 27 number of times applied. This is followed by the general deterrence theory (GDT) which has been applied 17 times while the Protection Motivation (PMT) is also indicated to enjoy usage by many scholars involving study information security ten times (Lebek, et al., 2013). One other common theory that has been extensively used in other areas of information technology is the Technology Acceptance Model that defines how users accept and embrace any new technology that has been applied 7 times.

2.5.1 Reasoned Action Theory and Planned Behaviour Theory

Theory reasoned action (TRA) was first fronted by two psychologists namely Ajzen and Fishbein. The theory underscores one's actual behavior result from one's own intention to actualize the actual behavior (Ajzen & Fishbein, 1980).

As with the trend with any existing theories, theory reasoned action’s (TRA) underlying assumption is that one’s attitude on their subjective norm together with their behaviours is dependent on their intentions at that particular moment (Ajzen & Fishbein, 1980).

Theory planned behavior (TPB) is yet one other theory mostly applied in many psychology studies and widely seen as an emergent of the Reasoned Action theory (Ajzen, 1991). The underlying assumption for the Theory of Reasoned Action and Theory of Planned Behaviour however remains largely the same with regards to one’s intention to act or behave in a way (Ajzen, 1991).

False consistencies between components due to the awareness of the theory’s assumptions by people has been one of the major criticism of the theory of reasoned action (Mykytyn, JR. & Harrison, 1993). However, the authors also noted the model’s basic structure allowed for ease of integrating factors such as top organizational management, and peers. This, they contended, has been important in previous research works that dealt with information systems success.

Despite the criticism as indicated by Mykytyn, JR. & Harrison, (1993), TRA has continued to find its space in scholarly work in information system research when it comes to behavioral studies. Several constructs have been availed by different studies covering a wide range of areas of interest. Several studies relating to the process of embracing technology have been conducted to determine factors that influence users to accept online systems or accept technology using TRA. These studies have employed or modified available constructs to suit their context.

Theory of Reasoned Action (TRA) has arguably found its way across many information systems research realms especially those whose studies involve the Organizational aspect and Human behavioral aspects of information system research. The relationship between one’s intention to comply and the corresponding actual compliance can be argued to have a direct correlation (Pahnila, et al., 2007).

Several studies have also gone ahead to combine several theories in one study. For example, a study on information security policy for employees conducted empirically Pahnila, Siponen, & Mahmood combined several theories in their studies namely *Protection Motivation*, *General*

Deterrence, *Reasoned Action*, *Innovation Diffusion,* and *Rewards* theories (Pahnila, et al., 2007). The constructs for Theory of Reasoned Action in their study included Intention to comply and Actual compliance. In testing their hypothesis, the authors concluded that based on their results, the actual compliance received a statistically significant influence from intention to comply.

Another similar approach to combining several theories was taken by (Gundu & Flowerday, 2013). In their study, the authors combined the Protection Motivation, Reasoned Action, and Behaviourism theories to study the role played by awareness creation to improve information security towards information assets in organizations. The authors noted the importance of Reasoned Action theory in explaining how employees' behavior towards organizational information security was influenced by the attitude towards organizational security as well the perception with regards to the corporate expectation of the employee.

In Information systems research, Planned Behaviour (TPB) theory can be found in many recent scholarly works as well as much older studies. One such studies is that of Bulgurcu, et al., (2010) in which the authors applied the TPB to study factors that contribute to compliance regime by employees with regards to information security policies whose findings revealed that one of the underlying basis of beliefs related to compliance was attitude (Pahnila, et al., 2007).

Similarly, a study by Pahnila, Siponen, & Mahmood also noted that social constructs of Planned Behaviour theory, within the context of awareness security facets, referred to perceived influence together with perceived motivation associated with the respective perception of the norm surrounding an individual (Pahnila, et al., 2007).

A combined approach of Reasoned Action Theory and Planned Behaviour Theory was also embraced in a study attributed to (Shareef, et al., 2009). Their research discovered a mediation of individual characteristics by beliefs which would then lead to an influence on attitudes. The attitudes also turned out to affect intentions and behaviours (Shareef, et al., 2009).

2.5.2 General Deterrence Theory

General deterrence theory appears to be numerously used behavioral theories in scholarly works related to information security (D’Arcy & Herath, 2011). Having started as a criminology approach to mitigating criminal behavior (Higgins, et al., 2005), GDT has been applied in many studies dealing with information security compliance (Pahnila, et al., 2007).

GDT bases its strength on rational decision making by stating that individuals’ decisions to commit crime balances the cost, and benefits of that crime based on the respective individual’s perceived severity, and the respective individual’s perceived certainty of sanctions or punishment (Lebek, et al., 2013). General deterrence theory applies punishment as a tool for preventing crime. Which in turn promotes required compliance by the whole society by creating conscious as well as unconscious inhibitions as preventive measures against crime (Kennedy, 1983).

In a study to investigate ways of converging user awareness and information security policies, Vaidyanathan & Berhanu, (2012) applied the general deterrence theory as a way to explore how the security countermeasures impacted the flow within an organization. The authors also applied GDT to explore the net effect there was on the organizational security performance, all these being moderated by security awareness.

Likewise, Schuessler & Windsor, (2009) applied the general deterrence theory whose results found an existing non-recursive relationship between threats and existing countermeasures. Further, the study revealed that the effective framing of the organization’s application can be achieved (Schuessler & Windsor, 2009).

Another application of the general deterrence study was from a study conducted by D'Arcy, et al., (2009) in which their deterrence theory model was extended to combine available theories from criminology, social psychology, and information system. In their work, they were able to conclude that there was a direct influence on perceived certainty from security awareness, as well as posit that there was a direct influence on information system misuse from how severe the sanctions were from organizations, which resulted in a reduction to misuse intentions (D'Arcy, et al., 2009).

2.5.3 Protection Motivation Theory

Having originally been proposed by Rogers, (1975) in which the author indicated that Protection Motivation Theory intended to provide understanding to fear appeals, a revision was made to extend the current PMT to Persuasive Communication theory. The proposition advocated more of the notion that behavioral shifts like appraisal threats and appraisal coping were mediated by cognitive processes (Rogers, 1983). As such, employees' motivation through awareness initiative is suggested to have worked in many organizations where compliance was enhanced (Veiga, 2015).

Equally works by Herath & Rao had earlier summarised that three elements provided a significant predictor of intentions to comply with policies. These were a combination of severe breach threat perceptions together with response efficiency perceptions, self-efficiency perceptions, and costs related to response which had a high possibility to impact on attitudes towards laid down policies; how organizations were committed and influence from social realms also significantly impacted on individual's intentions to comply; and availability of resource which appeared to have significantly influenced self-efficiency enhancement (Herath & Rao, 2009).

Protection Motivation Theory (PMT) has also been applied by various scholars within the context of relating information systems and by extension information security realm, and human or employee behavior. Several scholarly works apply the PMT theory in different ways and with varied constructs in their studies.

For instance, Sommestad, et al., (2015) applied the Protection Motivation Theory in a study that sought to understand ways in which information security stakeholders would appreciate the employee's understanding and the reasoning with regards to information security. The authors came up with Severity Rewards Vulnerability that tested the Response Coping, Threats, Self-efficacy, Response efficacy appraisal constructs. On the other hand, Kim, et al., (2014) looked at the Protection Motivation Theory from the response efficacy point of view.

Another application of Protection Motivation Theory can be found in the study of Mwagwabi, et al., (2014) in which they tried to look at how password guidelines compliance can be improved within organizations. In addition to Coping appraisal and Threat appraisal constructs employed by other authors, Mwagwabi, et al., (2014) introduced Exposure to hacking as a moderator to Perceived vulnerability which is one of the constructs under Threat appraisal.

In trying to address gaps that existed among the various socio-cognitive theories that have been employed to explain non-compliance by employees within organizations, Vance, et al., (2012) integrated habit alongside Protection Motivation Theory to explain the compliance phenomenon. There was a strong reinforcement of cognitive processes by habitual information security compliance as was theorized by Protection Motivation Theory in addition to future compliance intentions by employees (Vance, et al., 2012).

2.6 Behavioral Theories Application in Compliance-related Studies

Building on the theories in section 2.2 various behavioral theories, several authors have based their arguments on information security actual compliance or compliance intentions. For instance, Karjalainen, et al., (2013) opined that understanding the development stages of employees, cognitions of stage-specific barriers as well as impetus factors is vital to have a successful INFOSEC policy compliance practice by the employee. The authors expounded this by suggesting through their process theory whereby infosec policies compliance by the employees would follow a sequence of a varied stage in which there are associated stage-specific reasons for either compliance or non-compliance with INFOSEC procedures as well as barriers that produce and impedes the progression of the employee from a stage to the other.

Issues of trust within an organization have also been found to impact how employees interact with cases of incidents of a breach. If employees find it fine if they reveal what is potentially confidential information, then there is more likely that in the future, breaches will occur in that particular organization (Nabi, et al., 2014). This is especially if the employees feel justified due to the nature of the leak to their workplace involvement such as layoffs that organization management has been keeping a secret (Nabi, et al., 2014). Nabi, et al., (2014) also looked at trust and norms within an organization and their impact on information security (IS) policy compliance.

A look at other authors' approaches is that of Al-Omari, et al., (2013) who approached the compliance issue by basing their work on established scholarly work on psychology, information technology, as well as those that touched on business ethics. Out of these established works, they identified four behaviors of ethical nature. They argued that previous literary works did not satisfactorily scrutinize the role of different users exhibiting varied ethical ideologies in deciding on how to behave with regards to compliance, abuse, and piracy.

Al-Omari, et al., (2013), opines that ethical ideologies could be argued to have a significant influence in shaping the respective attitude of an employee with regards to complying with information security (IS) Policies. However, one among other limitations they identified was the generality issue since the location of the study was restricted to Jordan and this study argues that it would be interesting to find out what would emerge in other locations like in Kenya.

In trying to answer how organizational information security policies are understood, interpreted, or complied with by employees, David, et al., (2014) argued that for there to be effective compliance with information security policies, several measures had to be put in place namely, positive organizational culture, training, deterrence as well as job design. They further argued that this assisted the organizations in influencing the engagement by the employee as well as shaping the perception of the consequences and thereby improving the compliance with IS policies. They emphasized the need for organizations to have spelled ramifications of employees not complying and also ensuring that there is a clear guideline of how non-compliance behavior is determined.

Muhire, (2012) indicated positive as well as a strong relationship existing between employee's level of acquired education concerning information security (IS) awareness and with this in mind, it could be argued, implies that the more educated an employee is, the more aware they could be with relation to information security policies. Muhire, (2012) further argued that this level of education impacted positively the intent of the employees to comply. The assumption by Muhire, (2012) here was that a better understanding of the importance of policies and ramifications of not complying with organizational policies was a key contributing factor to enhancing compliance.

Hu, et al., (2012) on the other hand developed an information security employee compliance model that integrated three employee behavior-related models that are well established namely: support from top-level management, organizational culture, and planned behavior theory. Their study found out that top management involvement improved greatly the employee information security compliance through creating a robust organizational culture. However, they also contend that still more needed to be done to bring about a clearer relationship between aspects of organizational culture, aspects of organizational leadership, and processes that generate employees’ cognitions with regards to complying with information security (IS) policy by the respective employee.

Haeussinger & Kranz, (2013) concluded that information security (IS) Awareness has contributed some way in shaping employee's security behavior such that it could be argued that this could also influence the compliance by the employees to the information security policies.

Bulgurcu, et al., (2010) looked at the role played by cognitive beliefs on the attitude towards employee compliance. Towards this end, the authors found out that beliefs regarding overall consequences assessment had an immediate impact on attitude.

They argued that information security awareness exerted a significant positive impact on belief outcome and this further influenced the overall belief of the employees regarding the rewards of complying as well as the consequential costs of not complying all the while exerting a significant negative impact over belief outcome which often led to how the cost of compliance was perceived.

They finally recommended that attitude be included as a mediator in any theoretical model of information security awareness as a mediator having concluded by emphasizing the vital role played by the attitude in explaining beliefs assessment and relationships assessment including information security awareness and intention relationship

2.7 Grounded Theory in Information Systems Studies

As one of the mixed-method approach, grounded theory (GT) has been defined as a qualitative approach that consists of a systematic but as well as flexible guidelines applied in the process of collecting and analyzing qualitative data used in theory construction of which are grounded in data collected in the research (Charmaz, 2008).

2.8.1 Variants of Grounded Theory Methods

Though there may be other variants of grounded theory that are commonly used by researchers, three common ones are evident from extant scholarly work namely the Glaserian GT variant, Glaser & Strauss, (1967), Straussian GT variant, Strauss & Corbin, (1990), and Constructivist GT variant.

"Glaserian" Grounded Theory Variant

Since its initial development by Glaser & Strauss, (1967), grounded theory (GT) has intensively made its way and been used in scholarly works dealing with sociology fields especially in the 1960s in which many researchers adopted its use which included information systems research (Urquhart & Fernánde, 2013). It's from this that the "Glaserian" Grounded theory variant emerged.

Even though there have been a lot of arguments for not conducting prior literature work while applying the "Glaserian" GT approach, Urquhart & Fernánde, (2013) contend that this is a misconception that arises from the misinterpretation that researchers "MUST" start from a clean slate. The authors argue that for one to apply GT, literature forms part and parcel of the iterations and informs the next step through comparison though not as the primary data source for the next phase of data iteration (Urquhart & Fernánde, 2013). "Glaserian" GT approach has been argued to be exhibiting more of a scientific and positivist leaning that is no longer considered tenable (Bryant, 2003).

Straussian Grounded Theory Variant

The Straussian GT variant also referred to as qualitative data analysis as had been proposed by Strauss & Corbin, (1990) presents a point of departure from the originally developed GT by (Glaser & Strauss, 1967).

Strauss and Corbin highlighted a paradigm shift with regards to the coding strategy in which the researcher is supposed to look for contextual scenarios, prevailing conditions, action or interactional strategies in the environment the researcher is studying, intervening conditions of the research climate, and last but not least consequences which would guide the researcher on how to group and establish relationships emerging between codes (Strauss & Corbin, 1990).

The aspect of theory construction was however considered to acknowledge interpretive views (Charmaz, 2006).

Constructivist and Objectivist Grounded Theory Variant

Therefore, Charmaz, (2006) described Constructivist and Objectivists versions of GT in which Charmaz, (2006) argues that research applying the constructivist GT approach tends to prioritize more on incidents of the research and perceives the resulting data and respective analysis just as they originate from a mixture of experiences and relationships that are shared with those considered as participants as well as other data sources. On the contrary, Objectivist grounded theory, according to Charmaz, (2006) exhibits more positivist tradition in nature, and therefore instead of attending to the processes of data production, it concentrates on data as real. This study preferred the Constructivist grounded theory approach to its qualitative analysis.

"Interpretive" Grounded Theory Variant

A glimpse of Charmaz, (2006) works further discusses the inclinations of grounded theory with regards to the Interpretive phenomenon as well as Positivist. Interpretive theory gears towards conceptualizing the studied phenomenon to comprehend it in abstraction while articulating the theoretical assertions regarding the extent, deepness, control, relevance as well as acknowledging the subjectivity occurring in the process of forming a theory (Charmaz, 2006).

2.8.2 Constructivist Grounded Theory Process

Since this study leaned more towards the constructivism approach as highlighted by Charmaz for its first phase, it was best to investigate other approaches or models that had been proposed or applied in information system research.

One such approach was proposed by Gasson, (2004) who presented a collection of principles that would guide how grounded theory (GT) techniques are applied in qualitative research relating to information systems. Cognisant of the fact that grounded theory often faced criticism with regards to lack of rigor, Charmaz, (2006) emphasized the guidelines that advocated for; an inductive form of theory generation and emergence, formality of how a researcher may judge theoretical saturation, to what extent coding schemes formalization should be achieved, the debate regarding objectivist theory vs subjectivist theory approach and last but not least the assessment of interpretive research with regards to quality and rigor (Gasson, 2004).

Some of the steps enhanced by, Gasson, (2004) follows a systematic way in which everything starts by researchers conducting an open data coding to axial data coding after identifying core categories that can be extracted from the data, then theoretical memos follow immediately so that relationships and insights on categories captured (Gasson, 2004). Other subsequent steps involve "networks" analysis to extract and understand inter categories interactions as well as the respective emerging characteristics and lastly the step leads to substantive theory construction emerging after a rigorously conducted process of analysing the resulting patterns of the way core categories and how emergent network models eventually end up fitting new data (Gasson, 2004).

Several studies have applied grounded theory as currently existing in many scholarly works. However, many of these studies are found in other disciplines that are not Information systems related. Those in the information systems discipline have applied grounded theory as a way of validating rather than explorative study. Our exploration revealed that very few studies in the information security fields applied grounded theory. Our approach, therefore, considered grounded theory as an approach to data collection and analysis since it provides a better platform for theory development from qualitative method research. This study investigated a few of those research works that had employed Grounded Theories in other fields and limited the scholarly works to those that had dealt with organizational studies since this research also planned to limit its scope to the study of organizational culture dynamics when it comes to Compliance. This was important because looking at works already dealing with grounded theory and how they had been applied as well as how they had impacted the respective study; gave this study a locus standing to guide the data collection and analysis stages.

One such work was that of Martin & Turner, (1986) in which the authors argued that grounded theory was more applicable for researchers who would like to understand deeper the elements of the organization such as the corporate or organizational culture. The authors seemed to have adopted the strict grounded theory school of thought as championed by Strauss and Corbin. While endeavoring to understand the dynamics in organizations regarding the success or failure of Knowledge Management systems in organizations, Gupta, et al., (2000) also applied the grounded theory approach in the study. This is one of the applications of grounded theory in information system-related research.

In Organizational Studies, grounded theory as a methodology has also found its way as seen in the study by Ovaska, (2009) in which the author successfully assessed the role of organizational culture in information systems Development. Likewise, Stincelli & Baghurst, (2014) also applied grounded theory in their quest to investigate the perceptions of employees and managers on leadership qualities that occur informally in organizations. The authors argued for the adoption of grounded theory because, in their view, grounded theory provided a better way to analyze qualitative data in an exploratory environment as well as provide an ability to analyze data from various qualitative data points. Another notable grounded theory approach in the study of organizational culture was that of Kangas, (2009) in which the author applied mixed-method and triangulated the quantitative phase of the study with the grounded theory approach.

Researchers applying GT have experienced many challenges with regards to passing peer reviews due to mislabeling as highlighted by (Birks, et al., 2013). The authors indicate further that some researchers overcome the challenge by legitimately claiming that they applied only certain procedures developed under the GT framework as opposed to the method in the actual sense means that it's more than coding technics.

This study found its justification and comfort in applying GT in the qualitative phase from Birks, et al., (2013) that in their conclusion highlighted the flexibility of GT in the socio-technical realm of information systems such as is the case where this study tried to delve into the information security (IS) Compliance Culture context. The rigorous approach nature of GT as argued out by Birks, et al., (2013) was adopted and developed within the structures of needs of information systems research.

Further reasons why this study found it very important to apply GT in its qualitative phase was the compelling advantages given by Urquhart & Fernánde, (2013) in which they highlighted the relevance of the method since GT; they argued GT had a built-in close relationship with the data. The nature of the rigor that GT exhibit also forms a very important aspect to consider as part of this study since it had an elucidated analysis procedures, Urquhart & Fernánde,

(2013) and Birks, et al., (2013), this was an addition to clear and straight forward pathway to substantive theories generation. The authors also concluded and concurred with Birks, et al., (2013) that GT as a flexible research method would be ideal for researchers endeavoring to research on socio-technical processes as well as those endeavoring in theory building in areas that are relatively new in the scholarly which are very important to information Systems research.

As noted by Urquhart, et al., (2010) existing studies may be applied to formulate categories that may be useful in furthering grounded theory studies. This study, therefore, conducted intensive documentary analysis through the grounded theory approach. The resulting iterative data analysis and synthesis enabled initial categories to be identified. The emergent categories provided a rich source for interview guides to be administered in the main grounded theory methodology phase.

2.8 Empirical Review on Studies Covering Information Security, Organization Culture and Compliance

The approach above, as much as made sense within the context of a behavioral purview, what did not capture was how to inculcate the culture of compliance within the context of the strategies applied, something this study considers crucial for success in mitigating insider threat and for this reason, this study proposes a more comprehensive approach that combines many available compliance constructs to come up with insider threats mitigation strategy based on compliance regime.

Several models have been proposed by several scholarly works towards compliance such as (David, et al., 2014; Haeussinger & Kranz, 2013).

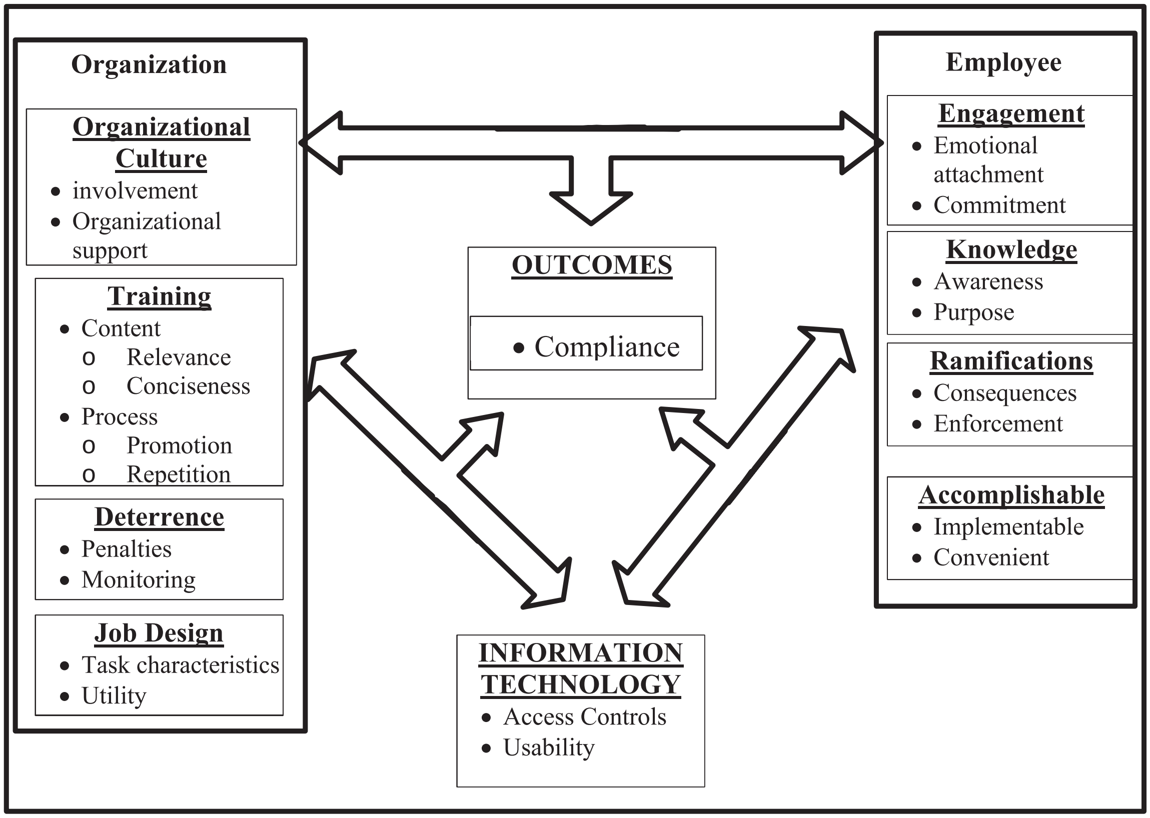


Figure 4: A model depicting how employees comply with information security strategies (David, et al., 2014)

As seen in Figure 4, an outcome of compliance was a function of information technology constructs organization constructs, and employee constructs. The study approached the compliance problem by looking at the relationships between Organization, Employee, and Information Technology. Based on their work, David, et al., (2014) provided very close interaction with the gap of this study which tries to address insider threat from a People, Technological, Organizational and Environmental point of view by providing the compliance version of mitigation from the first three constructs namely People, Technological and Organizational factors.

The study by David, et al., (2014) advocated for the creation of a supportive environment and systems within organizations that would have an impact on the perception of an individual employee on compliance behavior. They further discussed the role of Information Technology in the moderation of the relationship between organizational antecedents and individual employee cognitive elements whose net result would influence the compliance behavior of respective employees with information security laid down policies. In their conclusion, they averred that there was a relationship between organizational culture and actual compliance.

Scholarly work by Haeussinger & Kranz, (2013) also tackled the challenge of compliance by looking at it from Organizational, Employee, and Environmental approaches. Figure 5 shows relationships between Institutional (Organizational), Individual (Employee) as well as environmental factors on the general information security (IS) Awareness which then influences the way employees comply with security strategies. They argued that information security awareness formed the most important mediation of the relationship that occurs in antecedents of intentional behaviours to comply with information security policies. In the authors' view organizations need to take into consideration how they provide information security and how they factor in information systems knowledge by the employees.

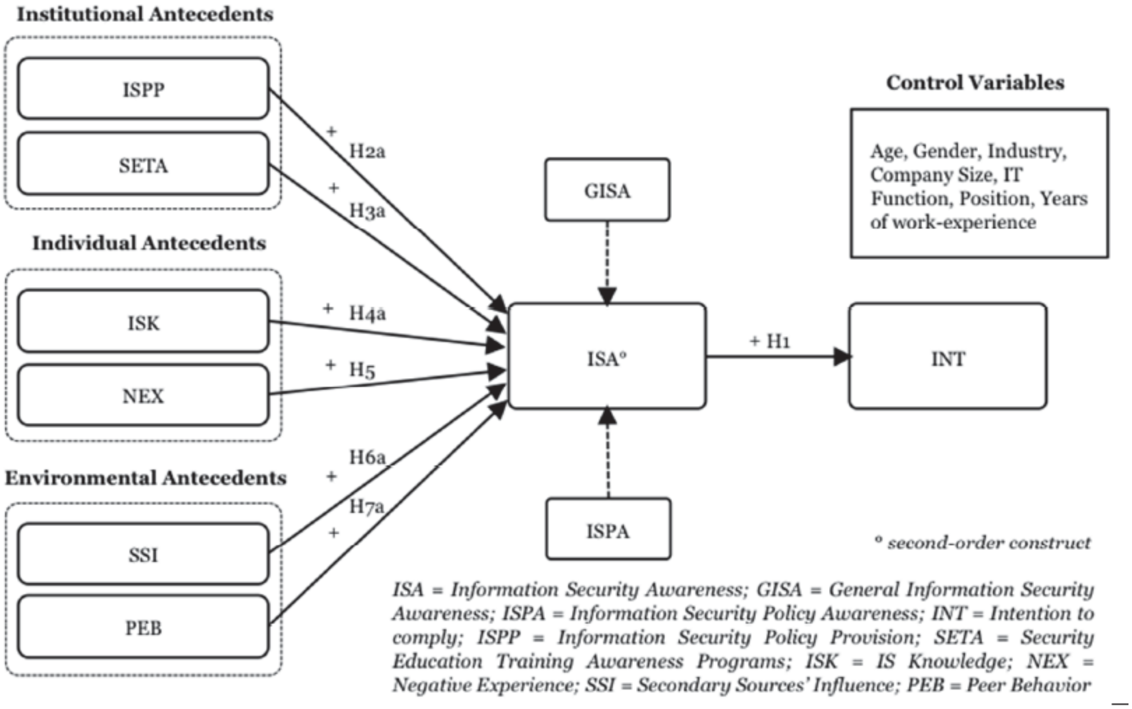

Institutional Antecedents
ISPP
SETA
+ H2a
+ H3a
Individual Antecedents
ISK
NEX
+ H4a
+ H5
Environmental Antecedents
SSI
PEB
+ H6a
+ H7a
GISA
ISA°
ISPA
+ H1
INT
Control Variables
Age, Gender, Industry, Company Size, IT Function, Position, Years of work-experience
° second-order construct
ISA = Information Security Awareness; GISA = General Information Security Awareness; ISPA = Information Security Policy Awareness; INT = Intention to comply; ISPP = Information Security Policy Provision; SETA = Security Education Training Awareness Programs; ISK = IS Knowledge; NEX = Negative Experience; SSI = Secondary Sources' Influence; PEB = Peer Behavior

Figure 5: A Model showing Information Security Awareness (ISA) antecedents and influence of ISA on information security policies compliance intentions (Haeussinger & Kranz, 2013)

Approaching from the context of a view of information system awareness was (Bulgurcu, et al., 2010). The authors proposed a model that considered compliance with an emphasis on a general attitude that made employees likely to comply. These were moderated by normative beliefs and self-efficacy to comply.

As already indicated Studies by Bulgurcu, et al., (2010) in which they also investigated aspects of compliance with information security by considering the Theory of Planned Behaviour as a basis of reasoning. They looked at factors that originated from rationality that could make an employee have a positive compliant behavior with regards to information system resources. Their findings showed that employees' attitude was impacted by the benefits, cost of compliance, and cost of non-compliance which could arguably be because of the consequences. One of the key things to note in their finding is also the important aspect of information security awareness which in their view, played a key role in shaping the effects and consequences of either complying or not complying and thereby contributed to the compliance behavior of the employees.

A study by Hu, et al., (2012) on the other hand considered the role of top management, organizational culture, and employee behavior and how they interact to shape compliance culture vis-à-vis the subjective norms and perceived controls attributed to employee behavior. In their findings regarding the relations that exist between the involvement of the top management, organizational culture as well as key elements that informs the compliance with information security policies by employees, they found out that indeed the involvement of top management with the information security programs significantly manifested direct and indirect impact on employees' general compliance behavior. Also, with regards to organizational culture, the authors found a relationship that existed between top management and organizational culture which also consequently influenced the greater compliance attitudes of the employees towards information security policies. A notable model is that from the authors was the outcome in which they tackled compliance topics from an only organizational point of view, Figure 7.

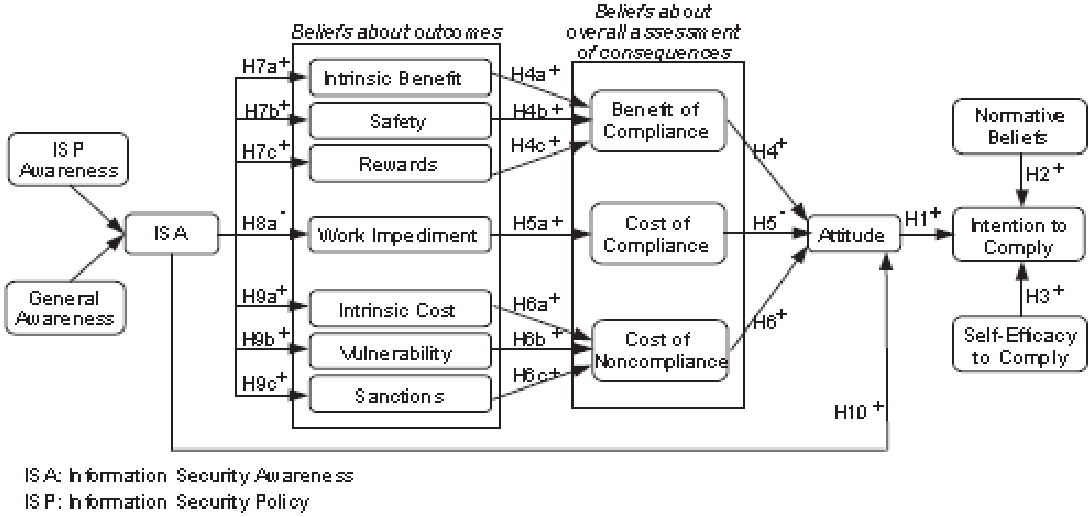


Figure 6: A Model depicting ISP Compliance Antecedents (Bulgurcu, et al., 2010)

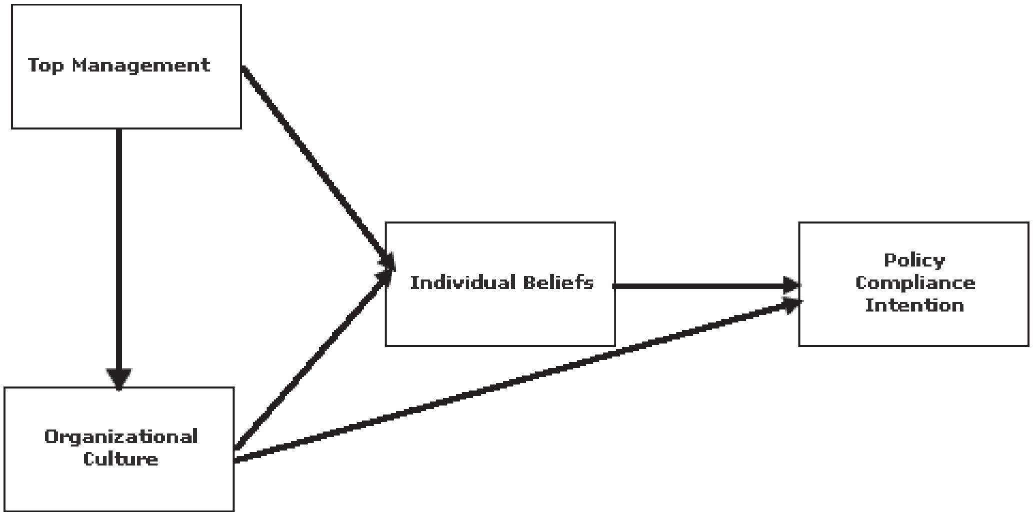


Figure 7: Conceptual model of individual behavior in organizations (Hu, et al., 2012)

A study by Chan, et al., (2014) on the other hand sought to understand the influence of common practices attributed to management and supervisors as well as the respective socialization by the co-workers on the perception of the employees of information security and the resulting security climate. The authors also investigated what contributed to compliant behavior vis-à-vis the security climate perception and self-efficacy. In their findings, they argued that there was a significant positive relationship between the existing practices from management and supervisors and perception of information security climate by the employees as well as the relationship between co-worker's socialization and the information security climate perception by the employees. They further proceeded to argue based on their findings that the said information climate perceptions and self-efficacy positively impacted the behavior compliance by the employees.

Figure 8 shows a model for employee compliance behavior proposed by Chan, et al., (2014) in which they looked at the relationship between Climate Observation of an Individual and information security climate perception when addressing the compliance behavior.

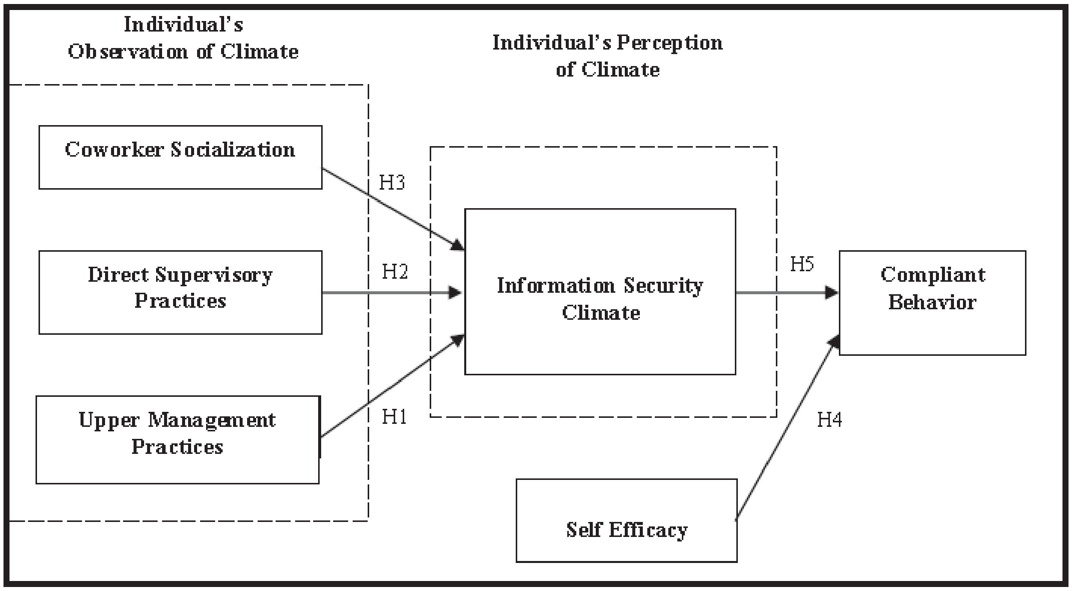

Individual's Observation of Climate
Individual's Perception of Climate
Coworker Socialization
Direct Supervisory Practices
Upper Management Practices
H3
H2
H1
Information Security Climate
H5
Compliant Behavior
H4
Self Efficacy

Figure 8: A Model for Employee Compliant Behaviour (Chan, et al., 2014)

With the background of all the models above, this study explored a model based on Organizational, Individual, Technological, and Environmental elements. These are the broad elements that this study proposed had an overall effect on the Insider Security Compliance Culture as a way of mitigating insider threats.

Another interesting model was the one proposed by Kam, et al., (2013) whereby the authors looked at higher education institution compliance with information security, Figure 9. Their findings suggested that there was indeed a significant influence on compliance with information security policies by the regulative pressure and social normative pressure which in turn can be argued to be able to shape the compliance behaviors of employees in an organization in higher education. This study also discussed further other approaches in the sections that follow to generate a conclusive working theoretical concept.

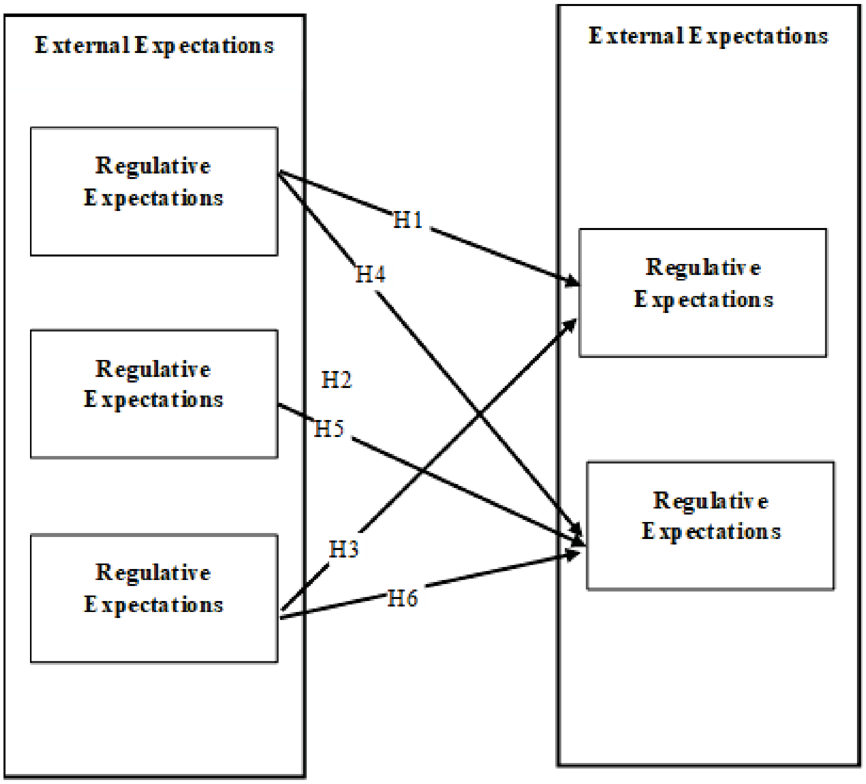


Figure 9: Information security compliance model in Higher Education (Kam, et al., 2013)

Other studies that have looked at the role of awareness, attitudes, beliefs, and habits with regards to information security behavior are the study by Pahnila, et al., (2007) that looked at information security awareness contributed significantly to the Actual compliance with information security. This was also in addition to their findings on the attitudes of the employees as well as their habits together with their normative beliefs which Pahnila, et al., (2007) argued contributed to the intention to comply. In their study, they also investigated the relationship between threat appraisals as well as the facilitating conditions. Their results revealed that attitude to comply was impacted to a great extent with the Threat appraisal as well as the existing facilitating conditions, further, they noted that coping appraisal was not of any significance when it came to attitude to comply with information security (Pahnila, et al., 2007). The authors further looked at the effects of sanctions and rewards for complying with information security and in their findings, the two had no significance at all with rewards not having any effect on actual information security compliance and sanction having no significance on employee’s intention to comply.

Another different view was taken by Karjalainen, et al., (2013) who took the approach of developing what they termed as a process theory. In their arguments, they elaborated that the process theory was to be used as an outline of various stages aimed at achieving behavioral compliance with information security. The authors stressed the importance of understanding the processes so that optimal mitigations are designed to improve the behavioral aspect of employees concerning information security. This, the authors argued, needs to be considered based on well-understood development trajectory together with stages that manifest themselves in behavioral aspects of information security as well as cognition barriers that are stage-specific and stimulus factors that equally stage-specific.

On the other hand, Nabi, et al., (2014) considered the question about what is considered as an acceptable norm by society even if all the employees are satisfied with regards to Information leakage causing a breach of information confidentiality. The authors argued based on their findings that an open policy in the organization regarding crucial information would help create trust and an environment that reduces anxiety. Top Management also has a role to play in creating what is accepted as the norms within an organization in addition to creating detailed plans about the responsibilities and the scope of the information technology section thereby improving on trust which the authors argued could play a very important role in shaping the compliance behavior of the employees in the organization (Nabi, et al., 2014).

Another approach with regards to the behavioral way of tackling information security was the approach taken by (Al-Omari, et al., 2013). In their study, they advocated for a model that considered the theories of planned behavior and ethics theory. Consequently, they identified ethical factors that in their views influenced the intention of the employees for complying with information security policies of organizations. One of their major points of emphasis was the greater importance of an ethical approach to enhance compliance with information system policy regimes within organizations.

Like the studies that discuss awareness was the study by Bertrand Muhire which also covered the compliance regime because of employees' levels of education. The study findings elaborated on the robust relationship that was positively identified existing the employees 'level of education and the level at which they manifested the awareness of the information security regime (Muhire, 2012). Further, they explained from their findings that the more educated an employee was the more the probability for the employee to understand and be aware of the information security policies and guidelines, and the more probable it was for the employee to comply. Therefore, it can be argued from their findings that the level of education played a role positively to the compliance by employees (Muhire, 2012).

While reviewing existing literature with regards to information security measures as practiced by organizations, Kaur, (2016) found that indeed employees and technology being employed by organizations had an important role to play when it came to ensuring that information assets are safe and accessible always.

Taking the behavioral approach also was a study by Best, (2014) in which the study looked at various tests to determine what caused the employees to comply with information security policies in one large company. The findings of the study found no influence by sanctions and self-efficacy but found that security awareness to have significant impacts on the employee's behavioral nature to comply. This was the case also with the top management support in which the study concludes to have a significant impact on the general employees' attitude towards complying and the actual compliance with information security policies.

From an organizational culture approach to addressing compliance behavior, Vroom & Solms, (2004) did a study in which they proposed several approaches to ensuring information security compliance in organizations. In their findings, they elaborated on the difficulties that exist in checking and accounting for human behavior which is crucial when formulating actions that touch on shaping human perception and behavior in an information security regime. They, therefore, argued that a culture changes through a much softer and informal approach be applied by organizations. This translates to organizations adopting a conducive and supportive environment just like the one proposed a few years later by (Best, 2014).

Approaching the issue of information security through the basis of interrogating the Confidentiality Integrity and Availability (CIA) triad, findings from a study by Chang & Lin, (2007) indicated that when an organization is effective and consistent in their internal information security operations, then the more they will succeed in the implementation of the information security basic foundations of Confidentiality, Integrity, and Availability. From information security management, the authors argued that effective and consistent operations affected positively the management of information system environments in organizations which in turn would generate a positive environment for compliance.

One other behavioral change proposition was done by Siponen, (2000) in which the author proposes information system security awareness and considered normative aspects of guidelines for end-users and respective guidelines for end-users. The authors considered and applied the intrinsic motivation behavioral science model and the theory of planned behavior together with the technology acceptance model behavioral science models to shed light on how behavioral role influences the behavior on information system management and came up with a model to address the role motivation plays in information security mitigations.

While acknowledging the shortcomings of various approaches existing which addresses the numerous threats that behaviours from employees might front in an organization, Veiga & Eloff, (2007) averred the need for organizations to consider comprehensive models that assist in cultivating security awareness culture. This is in line with many other studies that give information security awareness an important place in influencing employees' behavior in information security management within an organization.

Another behavioral consideration was found in the study by Herath & Rao, (2009) in which they sought to find out the influence that a penalty played in shaping the information security behavior in the organization among other aspects such as pressures that can be instilled on employees and the effective strategies of an organization. In their findings, they were able to deduce that indeed employee behavior was influenced by the normative belief that emanated from the management or superior employees and this impacted greatly on the compliance of employees with the information security policies (Herath & Rao, 2009). Of worthy to not is their further suggestion that given a situation where employees perceive the actions attributed to them would bring upon some different result which would be attributed to an improved security climate, then the employees' proceed to willingly be in support to the security policies (Herath & Rao, 2009). This implies that the possible success of the information security guidelines and policies would indeed assist in creating a following within the organization.

Looking at mitigation of information security and promoting compliance from the behavioral foundation, Chen, et al., (2012) also looked at the influence deterrence vis-à-vis reward and wage of employees, in which they averred that indeed organizations though their administrative structure could consider putting into practice the reward schemes and improvement of the wages control structures to place a positive response in the information security management. This was followed by the author's recognizing the crucial interactions that existed between punishment as a measure to deter wrongdoers and reward that encouraged the employees to look forward to benefiting after following the security policies as a way of improving organizational moral standing and considerations in ensuring information security compliance climate (Chen, et al., 2012).

As a way of also motivating employees to comply with information security policies, a study by Vance, Siponen, Pahnila found that components of the protection motivation theory that they considered influenced the intentions of employees into complying with information security policies within organizations (Vance, et al., 2012). They, therefore, concluded that indeed organizations needed to address the past and obvious behavior of employees to increase compliance rates.

One other observation regarding the actual compliance was made through a study by Siponen, et al., (2014) in which the authors looked into the role played by perceptions, attitudes, beliefs, and social norms within which employees exist within the context of information security management. In the findings of the study, Siponen, et al., (2014) the perception of how severe the threat of a potential information security incident can influence the intention of the employees to comply. This is also the case with the attitude of an employee towards compliance and the belief the employee holds regarding the application and adherence to information security policies. Likewise, the authors found that indeed social norms also influenced how much the employees intended to comply. In summary, they deduced that the actual compliance was significantly influenced by information compliance (Siponen, et al., 2014).

While looking into literature reviews and further conducting extensive exploratory interviews in three case studies, Alfawaz, et al., (2010) made findings that indicated factors that influenced behaviours of information security in organizations. They averred that indeed the values relating to national culture had some impact on information security behavior just like was the case with organizational culture.

Considering what their study considered as key components of information security management, Parsons, et al., (2015) identified a few important components namely awareness of policies, behavior that is brought forward by self and procedures as well as policies attitude by employees. In their findings, they found that indeed there was a significant relationship existing between decision-making outcomes on the security and information security culture of the organization.

Social bonds created in an organization, influences emanating from social set up in an organization, and the cognitive processing was the theoretical lenses adopted by Ifinedo, (2014) to discuss the compliance phenomenon as opposed to other numerous existing studies that have based study on information security compliance on deterrence theory. Ifinedo, (2014) avers in the study finding that indeed social bonds and influences, as well as the cognitive processes of employees, greatly influence the general compliance behavior of employees.

2.9 Synthesis and Emergent Categories

Several variables and predictors of information security compliance behavior can be discovered in the extant literature of theories and application of the theories. From the literature, constructs can be categorized as those that are associated with the external forces, those that are originating from internal organizational elements, and those that are individually oriented.

Individually, constructs and external factors such as Mimetic Pressure, Normative Pressure, and Coercive pressures are perceived to influence how organizations carry out themselves. Collectively, external pressures and Organizational attitude, as well as management support, were found to have some influence on how individuals behave in an organization. Elements such as Awareness creation and an individual’s perception of threats as shown by many authors also influenced the net behavior of individuals. Threat appraisals and perceived risks on noncompliance equally were found to greatly impact an individual’s net behavior with regards to information security. All these have been condensed into a working theory for this paper to form its Theoretical Model as shown in Section 2.11 below.

2.10 Emergent Categories

Having looked in detail what was the status of studies regarding information security mitigation, policy compliance, and the related social behavior controls, this study consolidated the related factors that might influence the behavior of employees with regards to intention to comply or the actual compliance to generate a working theory for the study.

Appendix 6 shows the resulting categories from the comprehensive literature review. What can be picked from the extant work points to social and technological as well as organizational environment factors that either hinder or promote compliance with information security policies can be summarized as Organizational and Institutional factors, Employee Factors such as social and behavioral antecedents, Environment factors such as management commitments, and Information Technology factors. All these have different elements that either shape the employee’s attitude to comply, or the employee’s actual compliance, or the shared values and norms towards compliance culture. Therefore, Figure 10 demonstrates what this study constructed in its working theory from the resulting theoretical background as found in extant literature.

From the various models highlighted, four categories of variables as indicated in, *Figure 4 Figure 5 Figure 6 Figure 7 Figure 8 Figure 9* emerge namely; those that can be said to be environmentally instigated, those can be said to be individually instigated, those that can be said to organizational as moderators and those that can be said to be technologically instigated. Following the Charmaz approach, the preliminary qualitative data extracted from extant literature was summarized and the following antecedents emerged.

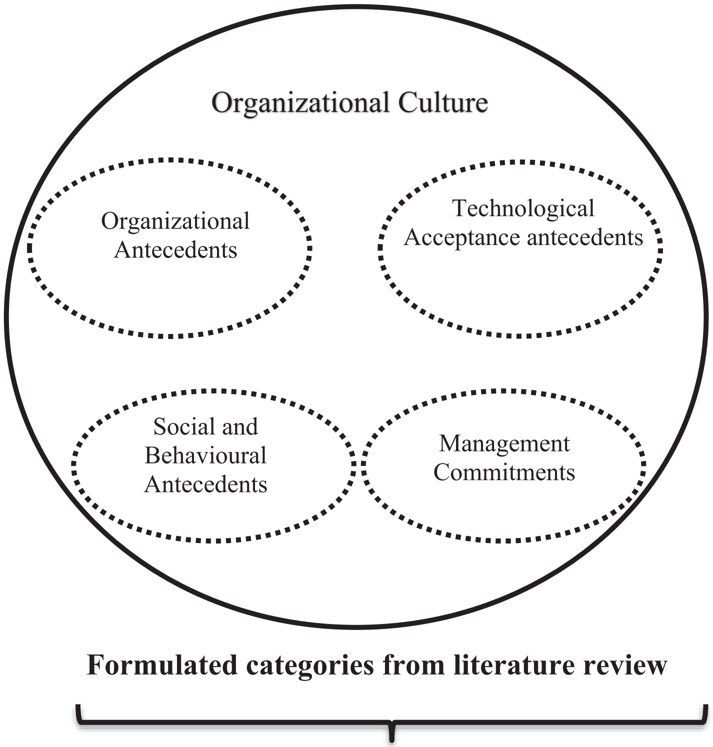

Organizational Culture
Organizational Antecedents
Technological Acceptance antecedents
Social and Behavioural Antecedents
Management Commitments
Formulated categories from literature review

Figure 10: Adopted Broad-based categories that contribute towards an established organizational culture

Organizational Antecedents

This category was defined by the organizational elements that shape its cultural practice. From the synthesized literature, this category was used to explore the organizational factors that define how information security compliance culture is nurtured.

Social and Behavioral Antecedents

This category was applied to define the broader explorative theme for individuals in an organization. Since the compliance aspect is more of individual action and may be shaped by other incidents of their social setup, this study considered the broader category as its explorative basis for information security compliance culture.

Management Commitments

From the synthesized literature, what emerged as a possible contributor to cultural practice in an organization was the commitments by the organizational management. The study, therefore, found a base to explore further management components of the organization and how they impact information security compliance culture.

Technological Acceptance antecedents

Adoption of technology by organizations also emerged to be a potential contributor to information security compliance culture. Technology acceptance antecedents appeared to shape how management and members of an organization perceived information security phenomenon. As such, this study found it necessary to explore further this antecedent.

As already highlighted in the definitions of organizational culture and organizational sub-culture, the four broader antecedents provided a broader approach for the initial lines of our query. Organizational culture has been variously defined by several authors as norms, values, artifacts, symbols, practices, rituals, control systems, power structures, etc. All these falls within one or two or all the four broad-based antecedents. As such, the relationship between information security compliance culture and the four broad-based antecedents would be through the prism of the broader organizational culture in which information security compliance culture is drawn.

As a recap, organizational sub-culture form when individuals come together and make interpretations of what are the norms, values, principles, and even generate artifacts and behavior based on their jointly common situations, identities, or job functions within their broader organizational culture (Hofstede, 1993; Denison & Mishra, 1995; Hofstede, 1998; Schein, 2004).

3.0 RESEARCH METHODOLOGY

3.1 Philosophy of Information Systems Research

There is consensus from scholarly peers that any research from any field needs to have the main tenets of what makes it sound research such as the ability to have specified the research philosophy of the study. These philosophies could be positivism, realism, pragmatism, or interpretivism. It is widely expected that any acceptable research needs to have reasons that inform the choice of the philosophical paradigm in question. This could be in terms of discussing the chosen research philosophy implications upon the strategy and the choice of primary data collection approach of the research. One of the definitions attributed to research philosophy is traced to Blaxter, et al., (2006), in which the authors described research philosophy as a belief concerned with how data regarding a phenomenon needs to be collected, analyzed, and utilized in the process of research.

Information systems research, just like any other research field such as health research, social studies research, etc., does have philosophical underpinnings or artifacts that define its realm. Several philosophies can be said to guide many studies that deal with information systems. Myers, (2008) opines that the scientific paradigm is the philosophical position that encompasses a researcher's underlying assumptions. These assumptions could entail various realities and knowledge which ends up influencing one's beliefs regarding valid and legitimate or justifiable research undertakings.

3.1.1 The Positivistic Philosophy

There exist several definitions of positivism as a philosophy. One such definition states that a positivist researcher bases his or her knowledge on naturally existing phenomena in conjunction with their respective properties and relations (Mingers, 2002). The Positivist research paradigm has mostly been applied in quantitative research undertakings although a few have been used in qualitative research as highlighted by (Goldkuhl, 2012).

Positivism as indicated by Villiers, (2005) has been equated to the scientific method, in which knowledge discovery is achieved by the controlled empirical way, with experiments as an example. Further, Villiers, (2005) contend that the intention of Positivist research is geared towards the generation of an exact representation of reality that is unbiased as well as value-free with reliable, and consistent results which have to be disentangled from any biases attributed to the researcher (Villiers, 2005). Primarily, researchers are reminded that positivist research is supposed to rely on quantitative methods, whereby data encompasses numbers as well as measurements while statistical methods are applied as a way of analysis (Villiers, 2005). Lastly, Villiers, (2005) indicates that results emerging from positivist research may be employed in cases where prediction is needed, and more importantly, that the studies are frequently hypothesis driven.

3.1.2 Interpretivist Philosophy

Relativism is argued to be the ontological stand on which interpretive philosophy is based (Guba & Lincoln, 1994). The main objective of interpretivism is to originate interpretations based on the research or underlying meanings emerging from the research while adhering to ontologically based assumptions exhibited by multiple realities (Villiers, 2005). This is while considering dependencies both in terms of timeliness and contextual realities. Interpretivism, as argued by Villiers, (2005) is also considered as an appropriate paradigm for researchers who study complex human behavior as well as social phenomena. Guba and Lincoln aver that relativism expresses the views that multiple realities are subjective and that there is a marked difference in the views from person to person perspectives (Guba & Lincoln, 1994).

According to Creswell, researchers who consider adopting interpretive methodology do so with the intention mainly to understand an individual’s perspective phenomenon, and considering an investigation of the interactions that exist between historical, cultural, and individual contexts in which people live (Creswell, 2009).

While discussing the strategic approach that students need to consider while adopting interpretive research, Walsham draws attention to critical elements of interpretive philosophy that any researcher needs to consider especially those at the Ph.D. level. Of key importance to factor in by researchers is the combination of such factors as; data collection approaches, data analysis approach, theoretical background, and in some cases, the ethical and moral issues that the research will be facing (Walsham, 2006).

Several methodology approaches have been adopted by researchers who have ventured into the realm of information system research. A case study can be argued to be one of the most frequently adopted methodologies based on extant literature.

3.1.3 Critical Realism Philosophy

Researchers who employ critical realism combine the generalized science philosophy with a philosophy originating from social sciences to give forth an interlinkage between the natural worlds and social worlds (Archer, et al., 1998; Mingers, 2002).

As opposed to positivism and interpretivism philosophies of information systems, Smith, (2006) argues that research work where the two philosophies were applied suffered persistent "…theory-practice inconsistencies…". Smith, (2006) continued to argue that the said inconsistencies could be identified between researchers' ontological assumptions concerning research practice, and in the results. It was from this premise of inconsistencies that Smith, (2006) proposed a critical realist ontology. Critical realist ontology allowed for a reinterpretation of activities emerging from scientific actions, that are founded on natural, and social realism in addition to conceptual ideas emanating from structures, and generative mechanisms therein.

Critical realism has been argued to provide a potentially better approach to social investigators who want to take advantage of its ontological provisions in terms of its analytical separation of structure and urgency (Dobson, 2001).

It is further argued that information systems research is fast embracing critical realism as an important component. Critical realism enables researchers to approach their research realistically while at the same time taking into consideration major inadequacies, and critiques emanating from a native realism school of thought (Mingers, 2002; Mingers, et al., 2003). Secondly, because critical realism embraces both natural science and social science elements, and since it has the potential to fit and blend with realities of both worlds as they exist in information system (IS), it is no wonder critical realism has been accepted in the IS world without a problem (Mingers, 2002; Mingers, et al., 2003).

3.1.4 Pragmatic Philosophy

In addition to Positivist, Interpretivist, and Critical realist philosophies that have been widely applied to information system research, Pragmatic philosophy has gradually found its way too into space (Goldkuhl, 2012). Pragmatism philosophy holds the school of thought that research can combine both extreme ends of the philosophies such as Positivist, Interpretivist and Critical realism all in one research. This implies that Pragmatism philosophy can be considered as both Inductive and Deductive, Goldkuhl, (2012) and tends to be case study-oriented (Mingers, 2002).

It is argued that researchers who apply mixed methods need to ensure that whichever method and philosophy they work with, they would try to put together many components of qualitative and quantitative methodological contributions into real workable outputs, as such, Johnson & Onwuegbuzie, (2004), advocated for pragmatic approaches that give way for researchers to incorporate the traditional dualisms that purists have debated.

Critical factors of pragmatics are the recognition of possibilities leading to varied worldview interpretation and research undertaking, in addition to the acceptance that an entire picture can never be given by one single viewpoint (Saunders, et al., 2012). As such, the critical nature of pragmatics is the acceptance of the possibility of multiple realities.

An argument fronted by, Feilzer, (2010) shows that Pragmatism can be taken by researchers as a guide for researchers who would be hoping to adopt a grounded inductive research process or abductive research process. This, therefore, offering an enabling environment to enable researchers to manage the complex and messy challenges that social life brings in addition to encouraging a revival of an emerging sociological imagination of researchers.

This study adopted the Pragmatic epistemology in its research since the mixed method was applied. As argued by Feilzer, (2010), Pragmatism can be supportive of various research method approaches in addition to approaches to analytical and reasoning behind it. Feilzer, (2010) further argues on the positive traits of pragmatism with regards to research design in addition to having a grounded foundation to research. This study was both deductive and inductive in principle.

3.2 Research Design

This study was an exploratory sequential mixed methods design. The study employed an exploratory approach in its first phase and a confirmatory approach in its second phase. The mixed method has been applied in the past by many researchers where there was no known phenomenal and contextual understanding of the subject research questions. Additionally, mixed methods have been applied by several types of research both in social and behavioral science and are quickly picking pace in the realm of information system research.

Triangulation of one's research results is often the most common reason for a researcher to consider mixed methods and thereby ensuring validation. This was the reason this study also considered applying a mixed method. Extant scholarly works indicate that mixed methods have on some occasions been used as a way of validation of the research by application of both qualitative and quantitative approaches. This argument is further strengthened by Howe, (2012) whose article concluded that there weren't any barriers to qualitative and quantitative methods triangulation. Literature also indicates that there are several reasons given by other researchers for choosing mixed methods as indicated by (Lopez-Fernandez & Molina-Azorin, 2011). Through their literature review study, the authors argued that development, triangulation, complementarity, and expansion could be considered as reasons for adopting a mixed method.

Based on the existing literature on the application of mixed methods, different research works differ on which approach between qualitative and quantitative is given more weight. Some have given more emphasis on quantitative than qualitative (QUAN + Qual), while others have put more emphasis on qualitative than quantitative (QUAL+ Quan). Others on the other hand have given the same emphasis on both qualitative and quantitative methods (QUAL + QUAN). All these different applications depend on what the researcher wants to achieve and depending on the research questions and objectives (Peng, et al., 2011).

Statistical validity has been previously used by several researchers as a way of validating qualitative research. Exploratory research, which this study applied, involved conducting data exploration whose sources originated from a documentary analysis in the pre-questionnaire stage, and semi structured in-depth interviews. The results were then restructured to a structured questionnaire to have statistical data as a triangulation approach.

This study gave more emphasis on a qualitative method to empirically collect and analyze data and used quantitative methods to validate the research in a sequential manner rather than a parallel manner and therefore started with the qualitative method. This was because the study was of exploratory design.

To address the critical informed anonymity consent, participants were informed on the objectives of the study and clear rights to voluntary participation or withdrawal addressed. The consent was given by the participants based on the research not disclosing the identity of the participants. To this end, the study ensured all was done to ensure anonymity by using identifier pseudocodes for both institutions and participants under the study.

This study was divided into two main phases namely phase one which covered the model development phase and phase two covered the model validation phase. **Error! Reference source not found.** demonstrates the workflow within both phases. Phase one of the study applied the Purposive sampling technique with grounded theory as the main methodological approach. While Phase two adopted a structured questionnaire. More details of each phase have been elaborately covered in the subsequent sections, 3.4 and 3.5 .

Diagrammatic Workflow Phases of Research Study

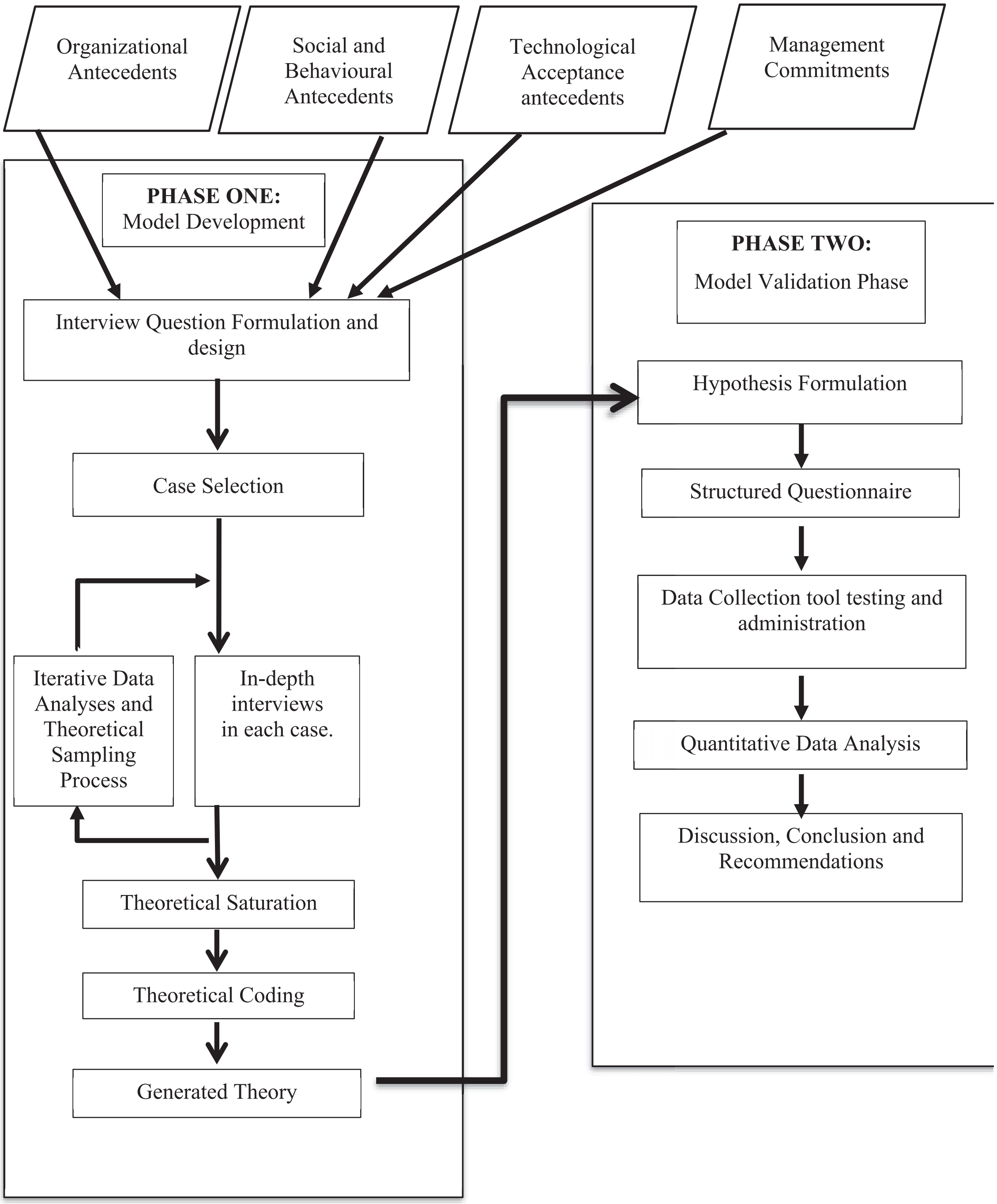

Organizational Antecedents
Social and Behavioural Antecedents
Technological Acceptance antecedents
Management Commitments
PHASE ONE:
Model Development
Interview Question Formulation and design
Case Selection
Iterative Data Analyses and Theoretical Sampling Process
In-depth interviews in each case.
Theoretical Saturation
Theoretical Coding
Generated Theory
PHASE TWO:
Model Validation Phase
Hypothesis Formulation
Structured Questionnaire
Data Collection tool testing and administration
Quantitative Data Analysis
Discussion, Conclusion and Recommendations

Figure 11: Diagrammatic representation of the Phases of Research starting from Phase one and leading to Phase two

3.3 Population and Sampling.

This study considered its population to be chartered universities in Kenya. The study extracted the chartered university list for the Commission for University Education website for its population. Table 2 indicates a total of **74** Universities authorized to operate in Kenya by the Kenyan Authority. Out of the **74** Universities, only **31** are publicly chartered and only **18** are Private chartered Universities. This study considered only the Public and Private Universities that already have the charters. That made the total population to be **49** Universities.

Table 2: Table showing the Status of chartered universities and their constituents and their numbers in each category (The Commission for University Education, 2017)

University Charter status by Institution's Type	**Count**
Public Chartered Universities	31
Public Constituent Colleges	6
Private Chartered Universities	18
Private Constituent Colleges	5
Institutions with Letters of Interim Authority	14
Total	74

This study conducted a preliminary data collection to give directions on the sampling frame for the grounded theory stage. The preliminary data collection was geared towards identifying only cases that could offer in-depth knowledge of the organizational culture and information security compliance culture.

To this end, the study considered that for such a sampling frame to be a viable option, it had to be a University institution that has already been chartered and has already instituted an information system related policy in place. This criterion was important because it gave the study an authoritative list of the population to be studied both in the qualitative phase and the quantitative phase.

A second criterion applied by this research to select a sample frame was to ascertain if the charted Universities had their respective information security-related policies in a public platform and accessible to all. This was done by going through the public website to search for the respective policies. For those that did not have the policy in the public portal, a secondary communication was initiated to seek knowledge of the availability of any such policies.

The third criterion was based on the duration the policies had been in place. This was important because for a study that seeks to understand the compliance instances and the organizational culture element, the longer the duration the better the findings would be.

The fourth criterion was the willingness to participate in the research. For the universities that had met criteria one, two, and three, a request letter was sent to each university requesting permission to conduct an interview, **Appendix 2,** and **Appendix 5**. Based on the three criteria, the study settled on The University of Nairobi and the United States International University.

3.4 Phase one: Model Development Population Sampling and Data Collection

Phase one addressed the research objective one and objective two. Research objective one was to explore the relationship of the factors that exist between organizational culture and the actual information security compliance in universities in Kenya. Research objective two, on the other hand, was meant to provide an explanatory aspect of these relationships through the generation of a theoretical model. These two objectives, therefore, relied on a qualitative approach to achieve the objectives. A double-case study approach was adopted for the data collection strategy in the qualitative phase. Qualitative data collection techniques and grounded theory methodology were applied to analyse the emerging theoretical data. In-depth interviews were adopted with an interview guide as the basis of the questions.

3.4.1 Research Design in the Qualitative Phase

The research adopted a grounded theory as the preferred research design in exploring the populations in the universities which were selected through Purposive sampling. We considered the case study approach as a model to have an effective in-depth interview plan. Interview questions were designed to answer the thematic aspects of the Theoretical concepts. The data collection and analysis followed the principles dictated by the grounded theory approach.

3.4.2 Grounded Theory (GT)

This study adopted the grounded theory (GT) process as proposed by Gasson, (2004) that followed the following sequence; ***Data Collection, Open data Coding, Axial data Coding, Theoretical Memos, Selective data Coding, Research Iteration, and Constant Comparison and then Progressed from Substantive theoretical model to Formal Theory***. This approach abided by the norms of grounded theory (GT) as envisaged by Strauss & Corbin, (1990) of multiple stages of data collection, data refining, and data categorization.

3.4.3 Data Collection

For initial data collection, an open-ended interview guide was used as drafted in **APPENDIX** 1 to get the emerging categories that were then used to inform the next stage of iterative data collection. Several data collection methods exist for studies implementing qualitative research. These may include observation, interviews which can either be an individual form of interview or focus group kind of interview, and a documentary analysis which can either be in text format or electronic and visual format.

3.4.4 Data Collection Process for Phase One of the Qualitative Iterative Grounded Theory Process

We factored in several critically important quality assurance practices to keep up with grounded theory procedures and principles in general of qualitative research. The processes and procedures are described below on what this study considered crucial to achieving quality.

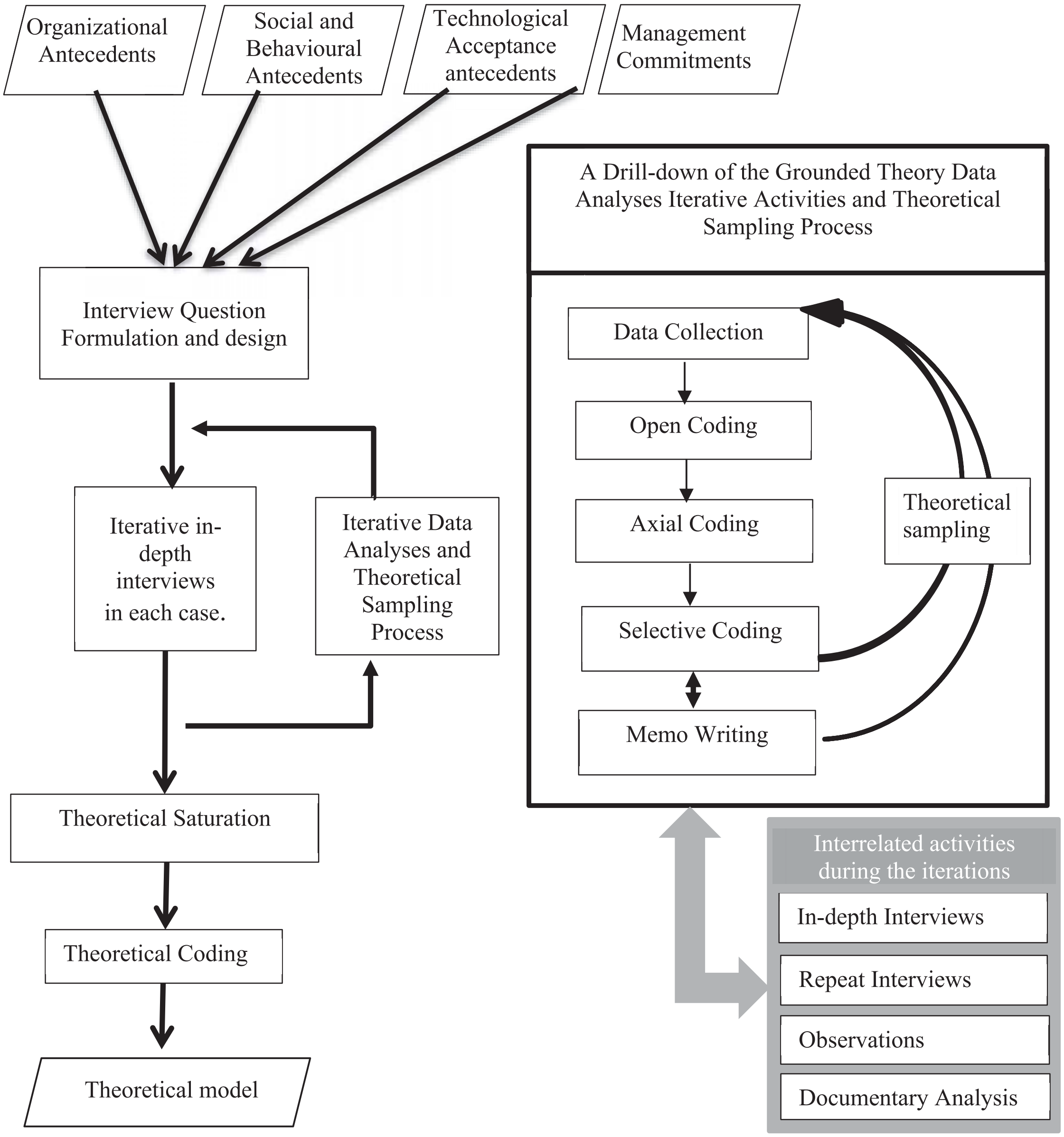

Organizational Antecedents
Social and Behavioural Antecedents
Technological Acceptance antecedents
Management Commitments
Interview Question Formulation and design
Iterative in-depth interviews in each case.
Iterative Data Analyses and Theoretical Sampling Process
Theoretical Saturation
Theoretical Coding
Theoretical model
A Drill-down of the Grounded Theory Data Analyses Iterative Activities and Theoretical Sampling Process
Data Collection
Open Coding
Axial Coding
Selective Coding
Memo Writing
Theoretical sampling
Interrelated activities during the iterations
In-depth Interviews
Repeat Interviews
Observations
Documentary Analysis

Figure 12: Illustrative diagram showing the detailed flow of activities during the iterative grounded theory process for the model development phase

The narrative for the Elements in *Error! Reference source not found.*

- **Open Coding -** In this process, we broke down, examined, compared, conceptualized, and categorized data into thematic categories. (***APPENDIX 10: Open coding stage***)

- **Axial Coding -** We invoked a set of procedures whereby data were reorganized in new ways after the open coding process. This was achieved by making connections between emerging categories. (***Appendix 11: Memo 4***)
- **Selective Coding -** In this stage, we selected the core categories and systematically related them to other categories, while validating the emerging relationships, and filling in categories that need further refinement and development. These were then recorded in the next phase of memo writing. (***APPENDIX 9: Selective coding stage***)
- **Memo Writing -** In this stage, we constantly recorded the experience, the emerging categories, and conditions in handwritten format and word document with comments. This was while applying a constant comparison approach to determine whether the category has an observable data saturation to be considered as a theme, or if new categories have emerged that need further unraveling, and what questions to ask as well as who to target next. (***APPENDIX 11: Constant memoing excerpts***)
- **Micro-ethnographic Process** – we conducted observations on a specific group of interviewees whom we engaged to identify cues and behavioral artifacts that formed part of our analysis. For example, we delved deeper into what was observed while talking to a group of students on the way to interview the planned 7th informant, and this was about the common observable behavior of "*not walking on grass*". This was what transpired:

  > "*…I believe that culture plays a very important role in shaping other cultures in any society. When I came in for the first time, I noticed that the students and staff had some form of way of life that was well established. I had no choice, but to conform. The university has several ways of nurturing the new members to feel part of the community. As you have observed, if you walk around, you will realize that no one walks on the grass to create short cut routes. Everyone is conscious of what the colleague will see or say about them. And I believe that this is what creates an element of compliance with information security policies as well in the university….*" **Informant 7: ICT-Staff - University A**

- **Theoretical Sampling** – This stage represents the net process after collecting all the codes and the resulting data analyses leading us to determine which data needed to be collected next, from whom to extract them, and the questions to be modified to reach the goal. It is at this stage that determination was made to identify which deviant cases we should pursue more. For example, once it started emerging that the students were becoming more and more relevant as opposed to the faculty and IT specialists as initially perceived, we decided to consider the students as the deviant groups next. It was at this stage also that decisions on the sample size adjustments were considered based on the selective coding and memos

- **Theoretical Coding –** As a final stage before theory generation, we proceeded to last iterative theoretical coding, while traversing through the data after observing the theoretical saturation. This was done to explore the conceptual reintegration of themes into a theoretical model as an outcome. (***APPENDIX 8: Theoretical coding***)

Data Collection Strategy in Summary.

1. We recorded digitally all face to face interviews for those interviewees who gave consent to be recorded.
2. Thereafter, we transcribed in detail professionally and checked all the transcripts against the recordings.
3. The interview transcripts were analyzed after each round of in-depth interviews where possible and thereby enabling theoretical sampling to occur.
4. By jolting down case-based memos immediately after each interview, and while still within the field environment, we were able to capture initial observations and ideas and thereafter make important comparisons between the narratives of those we interviewed. This took the form of ***micro-ethnography***. This enabled us to construct our reflections and thereby enrich our data analysis as well as further data collection strategies.
5. We also indevoured to contact participants after interviews in a bid to clarify concepts. The back and forth to interview the interviewees several times contributed to the refinement of the emerging theoretical concepts and thereby supported the part of theoretical sampling.

Data Analysis

We employed the use of the constant comparative approach that enabled the analysis to generate a description and a theoretical model.

3.4.1 Population Sampling

The population size to be interviewed varied markedly when the grounded theory approach of the Qualitative Method is applied. Theoretical saturation is said to be the determining factor of what sample size is sufficient to project clear patterns, concepts, categories, properties, and dimensions (Thomson, 2011; Mason, 2010).

The question that arose therefore was "*What would be the reasonable sample size to interview that guarantees unquestionable saturation point*?" This question is partially addressed by Charmaz, (2006) in which the author argued out that for some types of small projects, a modest 25 interviews may seem to be enough. Although the researcher may invite skepticism from peers when the author's claims are about, human nature or if the outcome contradicts established research. Theoretical saturation should be what grounded theorists focus on (Charmaz, 2006).

On the other hand, Mason, (2010) contends that the average sample size could be taken as 31 respondents. Mason, (2010) however notes that there was a non-random distribution with statistical significance of some studies presenting multiples of 10. Similar findings were seen from a study by Thomson, (2011) in which the results indicated that even though a sample size of 25 was average in all the work studied, 30 interviews were best recommended if one was to succeed in meeting the principles of grounded theory such as pattern development, concept development, deriving of categories, properties identification and generating the various dimensions of a particular subject matter. It was also noted by Francis, et al., (2010) that qualitative studies may also be considered okay with a minimum of 13 sample sizes. Theoretical sampling together with theoretical saturation could provide some level of solidity for the emerging analysis and thereby assist in keeping it grounded on empirical qualitative data. This study observed data saturation at the 20th interview and therefore fell within the reasonable accepted sample sizes based on the existing works.

3.4.2 Case Selection Criteria

The first phase of this study dealt with Theory generation thereby calling for a sample population that could avail in-depth data focused on a specific area of interest. The choice of sample to be studied therefore needed to be selected through a non-probabilistic sampling technique such as Purposive sampling. Several sampling techniques have been considered by researchers based on the nature of the population they are intending to deal with. This study adopted Purposive sampling since the area of interest was already narrowed down. This is in line with what many researchers have adopted and whose work aimed to obtain a more in-depth understanding of a typical case under study as opposed to the need for generalizing research findings (Neuman, 2009).

As already hinted above, to get the desired case, universities' public websites and portals were searched to see if they had information systems related policies in place. Those that did not have any information systems related policies on their website were contacted to request their assistance in acquiring the policies where possible and to seek further information. Out of the 31 Chartered public Universities, only 7 Universities had their information systems related policies in place and available on their websites for access. Out of the 18 Chartered private universities, only 2 universities had their policies on their websites and available publicly. Those that already had policies in place and available in public were noted and an email was sent to request further information and to get their consent in participation in further research engagements. Appendix 2 shows both the letters sent to Universities that had policies accessible to the public and those that did not have policies accessible to the public.

3.4.3 Case Study

Case studies have been applied in research works where the main objective is new theory building, testing of existing theory, and in cases of evaluation of alternative theories (Oates, 2005). Case studies and grounded theory have been considered to complement each other based on their strength and supportive of their weaknesses. Although case study has been critiqued as lacking the ability to generalize results, this has been addressed by many researchers by combining with grounded theory to provide some level of rigor while at the same time enjoying the in-depth aspect of case study (Taber, 2000).

One needs to consider the underlying philosophy to know whether the underlying philosophy applied is in sync with the case study before applying it since as indicated by Oates, case study as a strategy cannot be tied to only one philosophical viewpoint but can be applied in all the underlying philosophies such as positivism, interpretivism and critical realism (Oates, 2005).

This study, therefore, found it fit to apply the case study strategy cognisant of the underlying philosophy of interpretivism that already gives it impetus with regards to applicable philosophy.

Oates further elaborates more examples of advantages that case studies accords a researcher more than disadvantages especially for researchers who would foresee themselves dealing with complex situations in which single factors in isolation becomes very problematic: where researchers are considering theory building and experiencing little control over situations and events, where researchers envisage a situation where they would want to show life complexities and exploration of alternative meanings and explanations, or where researchers want data outcomes that want to capture close respondent's experiences which can be more accessible as compared to highly numeric studies (Oates, 2005).

Oates, (2005) further notes the disadvantages of case studies in which the author argues that case studies are criticized as lacking rigor and thereby contributes to poor generalization and credibility or that case studies can be time-consuming and very challenging when it comes to negotiation of how to access necessary settings, people, and documents. There is also a possibility of researchers getting respondents to change their behavior in their presence thereby not getting the result they expected. Another challenge is the lack of a set of rules to be followed as well as the inability for one to know before whether they are on the right path before the study goes too deep (Oates, 2005).

Notwithstanding the disadvantage, this study is convinced that all the disadvantages have been duly considered for the case study to be applied as its data collection strategy within the grounded theory methodological approach. This is achieved following Lincoln and Guba's criteria to ensure that adopting a case study as a data collection technique and grounded theory does not render research prone to critiques. According to Lincoln and Guba, although suitable mostly in positivist research, interpretative qualitative researchers also need to take into consideration certain evaluation mechanisms that will give some strength to their work (Lincoln & Guba, 1985). These include Credibility, Transferability, Dependability, and Conformability (Lincoln & Guba, 1985).

Although several studies had insinuated a priori sample size as would be the case with a case study, this research focused on grounded theory principles and considered no maximum number of interview batches in each selected case and, instead, increased the sample population as many as necessary until the point at which theoretical saturation was observed. This study sample approach was considered appropriate for the interviews by this study because it fitted between the already suggested sample size ranges as indicated by (Charmaz, 2006; Francis, et al., 2010; Mason, 2010; Thomson, 2011). The study considered two university cases one that met the criteria as already discusses under the selection criteria below.

3.4.4 Biases of Qualitative Research

Every researcher has had to deal with issues that raise the question as to the objectivity of the research due to biases from their thinking. This is more pronounced when applying qualitative research since most of the time data must pass through the researcher's prejudice. As a result, it is no surprise that critics of Qualitative research have given many reasons to question the methodology. The criticism has taken many forms such as scientific nature, objectivity, trustworthiness, reliability, and validity among other issues (Kvale, 1994; Shenton, 2004).

As noted by Rajendran, (2001) researchers have no option but to face their influences of biases to the data due to unavoidable opinions and prejudices. This calls for the need for the researchers to apply methods in processes that assist them in transcending their own biases that may exist (Rajendran, 2001).

3.4.5 The Trustworthiness of Qualitative Research

While studying the trustworthiness of the grounded theory method (GT) Sikolia, et al., (2013) suggested that by increasing the trustworthiness of the research, a researcher could in effect enhance the quality of GT. The authors further argued that the negative case analysis, data source triangulation, peer debriefs, audit trails, having a sharing session of transcripts with individual participants as well as having prolonged engagements involving informants can act as a way of realizing increased trustworthiness.

A look at scholarly work involving health research and social research where lots of behavioral studies are done under the qualitative approach, questions of trustworthiness and validity have arisen and ways of dealing with these suggested. While researching a counseling psychology study, Morrow examined qualitative research concepts with regards to its trustworthiness or credibility and made suggestions for researchers planning to use qualitative research on how to increase trustworthiness (Morrow, 2005). One of the suggestions given as an example was the identification and explanation of each step of the coding and categorization when applying grounded theory.

3.4.6 Selection of the First Case and Second Case Unit of Study

As already highlighted in the case selection section, interviews were conducted in batches based on theoretical sampling principles. The interviews were conducted in approximately two and a half months with each interview lasting an average of 25 minutes. The interviews were broadly based on interview guides which were developed as a result of an emergent categories model as illustrated in Figure 10. The interview guide was further refined or modified after each batch to elicit theoretical sampling in line with grounded theory principles. A Non-verbatim transcription strategy was adopted. We employed the use of an online tool (oTranscribe, n.d.) to transcribe our audio interview recordings into a coherent and understandable flow.

3.5 Phase two: Model Validation Data Collection and Population Sampling

Phase two of this research was designed to address objective three. This was geared towards validating the emergent theoretical model from section 3.4 in a confirmatory factor analysis approach. A descriptive research design was adopted for this research phase. Hypotheses were developed from the theoretical model emerging from the section. Table 3 shows the individual hypothesis and the respective key indicators and coding. A structured questionnaire was adopted as a tool to conduct a survey. The online form was created on a google online platform. Appendix 7 shows the questionnaire that was used in the online google form. The questionnaire was targeted towards all staff and students of the participating universities.

Table 3: Hypothesis, Key Indicators, and Coding

Hypothesis	Key Indicators and Coding
H1: Age has a moderating effect between *Individual Demographic Interventions* and *information security compliance culture*.	• Mature staff are more likely to reason and comply with information security policies in place **(DMF-AF1)** • Handling a diverse age group provides a challenging environment when enforcing information security policy **(DMF-AF2)**
H2: Social upbringing to some extent influenced how users complied with information security policies	• The difference in social upbringing provides a big challenge when enforcing information security policies **(DMF-SU1)**
H3: Social pressure has a moderating effect between *Individual Demographic Interventions* and *information security compliance culture*.	• Handling members under seer pressure is challenging when enforcing information security compliance **(DMF-SP1)**
H4: Education background influences information security compliance	• We have challenges enforcing information security policy when dealing with members with a technology background **(DMF-EB1)**
H5: Management support has a moderating effect between *Organisational External Interventions* and *information security compliance culture*.	• Management support improves the execution of information security policies **(OMF-MS1)** • I feel motivated to comply with information security when management also complies **(OMF-MS2)** • It is easier to create awareness when management gets involved in the process **(OMF-MS3)**
H6: Regulatory authorities influence organizational initiatives towards information security compliance	• We are obliged to follow the regulatory authorities' requirements **(EOI-RA1)**
H7: ISO certification and standards influence organizational initiatives towards information security compliance	• External certification obligations increase the level of responsibility to enforce compliance with information security policies **(EOI-ISO-CS1)**
H8: Best practices from peers influence organizational initiatives towards information security compliance	• Learning from peers encourages a well-planned information security compliance initiative **(EOI-BP1)**
H9: Awareness program initiative by organizations influences the compliance with information security policies	• A conscious society increases the level of compliance with information security policies **(OS-AP1)**
H10: Capacity development initiatives by organizations influence information security culture	• Constant training and capacity development encourage members to comply with information security policies **(OS-CD1)**
H11: The deterrent control initiatives by organizations influences information security compliance culture	• Our deterrent initiatives discourage noncompliance behavior **(OS-DC1)** • Our control mechanism reduces incidents of non-compliance with information security policies **(OS-DC2)** • Our monitoring initiatives enables the detection of information security breaches in time **(OS-DC3)**
H12: Perceived ease of ISP application influences the information security compliance culture in organizations	• I am more likely to comply when the policies are interventions are easy to understand and use **(IBT-PEIA)**
H13: Perceived risks of ISP application influences information security compliance culture in organizations	• I am more likely to avoid complying with information security policies if I perceive them to be a risk to me or my privacy **(IBT-PRIA)**
H14: Individual attitude influences information security compliance culture	• Rebellious members will more likely violate information security policies **(IBT-IA1)** • My attitude towards the policies will impact how I comply **(IBT-IA2)**

3.5.1 Construct operationalization

The constructs were then operationalized to enable the development of a questionnaire. Operationalization is important to any study because it helps to develop indicators or constructs that will be measured in the study. In operationalizing the constructs, we identified which constructs were reflective, which constructs were moderating factors. The nature of reflective operationalization was also identified in terms of whether they were negative or positive. Table 4 summarizes how the constructs were operationalized for the study.

Table 4: Construct operationalization

Constructs	Operationalization Type	No. Measured Items and Codes
Information security compliance culture	Reflective	
Age factor (Maturity Level) **(AF)**	Moderating	• **(DMF-AF1)** • **(DMF-AF2)**
Social upbringing **(SU)**	Moderating	• **(DMF-SU1)**
Social pressure **(SP)**	Moderating	• **(DMF-SP1)**
Educational background **(EB)**	Moderating	• **(DMF-EB1)**
Management support **(MS)**	Moderating	• **(OMF-MS1)** • **(OMF-MS2)** • **(OMF-MS3)**
Regulatory authorities **(RA)**	Reflective **(+ve)**	• **(EOI-RA1)**
ISO certification and standards **(ISO-CS)**	Reflective **(+ve)**	• **(EOI-ISO-CS1)**
Best practices from peers **(BPP)**	Reflective (+ve)	• **(EOI-BP1)**
Awareness program **(AP)**	Reflective **(+ve)**	• **(OS-AP1)**
Capacity development **(CD)**	Reflective **(+ve)**	• **(OS-CD1)**
Deterrence Control mechanisms **(DCM)**	Reflective **(+ve)**	• **(OS-DC1)** • **(OS-DC2)** • **(OS-DC3)**
Perceived ease of ISP application **(PEIA)**	Reflective **(-ve)**	• **(IBT-PEIA)**
Perceived risks of ISP application **(PRIA)**	Reflective **(-ve)**	• **(IBT-PRIA)**
Individual attitude, **(IA)**	Reflective **(+ve)**	• **(IBT-IA1)** • **(IBT-IA2)**

3.5.2 Sampling Design

This study adopted Cochran's formula in calculating the estimated sample size which has been considered in several studies dealing with an infinite population (Cochran, 1977). The choice to consider an infinite population was made with the assumption that it would be difficult to estimate the number of respondents in the selected university at any given moment.

$$s_0 = z^2\, p\, q \,/\, e^2$$

Where:

s_0 is the sample size, z is the selected critical value of desired confidence level, p is the estimated proportion of an attribute that is present in the population, $q{=}p{-}1$ and e is the desired level of precision.

Therefore, assuming our maximum variability was equal to **50% (p=0.5)** while considering confidence level as **95%** with **±5%**, precision, we calculated the required sample size as below.

$p = 0.5$ and hence $q = 1\text{-}0.5 = 0.5;\ e = 0.05;\ z = 1.96$

$$s_0 = (1.96)^2\,(0.5)\,(0.5) \,/\, (0.05)^2 = 384.16$$

s_0 Rounded off to the nearest 5 = 384

This study, therefore, estimated its sample population to be **384** respondents that were targeted.

3.5.3 Target Population in Quantitative Method Phase

This study considered 8 Chartered Universities both public and private as its target population. The universities were considered based on the longevity criteria of 20 years in operations. The choice of the target population was due to its diversity. This was deliberate since this study argued that for a more realistic generalization to be made from the results arising from this study, a wider and more diverse population needs to be considered. Some studies have argued that part of the limitation of their study is because of limited sample size (Kam, et al., 2013), and as such, this study found it necessary to target a much larger sample size by enlarging its target population respondents.

3.5.4 Pilot Study

A pilot phase was conducted by sharing the draft questionnaire with 10 respondents outside the participating universities. Data was collected using the questionnaire to test the instrument's validity and reliability and to determine the logic, clarity and objectivity of instructions and questions that appeared in the questionnaire. We also used the pilot data to check whether the indicated variables were easy to be analysed and interpreted for reporting and presenting the study findings. Information collected from the pilot study was not used in the final data analysis of the study but it helped us make decision that no changes were needed on the questionnaire, the strategy used in dissemination of the questionnaire and on the analysis technique adopted for the study. Respondents engaged for the pilot study were not included in the study sample of the main study.

Since the pilot phase did not show any difficulties in understanding the line of questions and went smoothly. The pilot respondents also indicated the research protocols were satisfactory. Besides, the data collection instruments emerged as meeting the standard as envisaged by the study. This outcome enabled the study to proceed with the data collection stage without any further modifications. Before the decision to continue with the questionnaire as is, we engaged experts in the information systems to determine if the line of questions would make sense and if the logic of the questions were truly going to answer the objectives of the study.

3.5.5 Data Collection Method

The study shared the online form generated via a google form to a few representatives within the participating universities. The representatives then shared within their networks and peers. The online form was considered because it offered a wider reach with minimal resource barriers while maintaining the anonymity of the respondents. Follow-up calls were made periodically to the first line of volunteers who also followed up with their network to enhance response rates. This approach of using trusted volunteers in the network to reach out to other trusted volunteers was deliberate due to the nature of the study. Since the study involved getting information related to information security behavior, there was a need to earn the trust of the respondents. By involving those who are known to other respondents, addressed the possible issues arising from lack of trust and thereby increasing the response rate. Out of the envisaged 380 responses, the study managed to garner a total of 364 respondents across 8 universities. To address concerns of biasness and sample representativeness, the study ensured anonymity in the process of accessibility to the peer networks. The assumption made was that the peer network would randomly share the questionnaires without prejudice. As such we were able to handle the concerns of biasness that would arise if the researcher would purposively select whom to give first-hand questionnaire in the data collection process

3.5.6 Quantitative Analysis Methods

The quantitative analysis design was developed as an extension of the exploratory sequential research design factoring in the emerging results from the exploratory phase. Accordingly, the study followed the approach that enabled the collection of data in the exploratory phase, and then proceeded to collect and analyse the data which was eventually used to develop the quantitative instrument to further explore the research problem as proposed by (Creswell and Plano Clark 2011; Onwuegbuzie, Bustamante, and Nelson 2010). As an explanatory sequential research design, a strategy to analyze the data and ensure model validity and reliability were adopted based on exiting works that have experienced exploratory sequential type of research. To this end our study partly borrowed the approach by (Berman, 2017) in the design of the second phase in terms of the validation and reliability tests. Consequently, as part of the analysis design, the study adopted factor analysis, chi-square test and Cronbach's alpha tests for the validity and reliability tests.

This study adopted a Confirmatory Factor Analysis (CFA) approach to validate the emergent model. CFA has been found applicable to a variety of research analysis needs such as construct validation, as well as evaluation of measurement invariance (Brown, 2006). The same approach had also been taken by Shafiu, et al., (2016) in which the authors looked at information security compliance behavior in a food chain security. This study adopted the CFA approach because of its power in allowing hypotheses testing by researchers on certain factor structures. CFA has been considered to produce numerous measures for goodness-of-fit that enables model evaluation as opposed to factor scores (Albright & Park, 2009). CFA has also been used by researchers to test a proposed theory as was the case with this research (Williams, et al., 2012).

4.0 RESULTS AND DISCUSSION

This chapter highlights the results and discussion of the qualitative phase and the quantitative phase. The section addresses the objectives of this study under the model development phase and the model validation phase. In the model development phase, the objectives were an exploration of the relationship that exists between organizational culture and the actual information security compliance in universities in Kenya, and the explanation of the relationships that emerges with the model. In the model validation phase, the objective was to validate the emergent theoretical model in phase one. This section also discusses the results in both phases. The section is divided into the results subsection and discussion subsection. The objective was to validate the theoretical outcome with a Quantitative approach.

4.1 Model Development Phase Results

The study observed data saturation at the **20th** interview and therefore the researchers concluded conducting further interviews because no more categories were emerging. The researchers were satisfied with the 20th interview point at which the data saturation was observed because it fell within the acceptable sample size for grounded theory. This was also in line with earlier highlighted sample size ranges as supported by (Charmaz, 2006; Francis, et al., 2010; Mason, 2010; Thomson, 2011). The rationale for data saturation at the 20th interview was also supported by Preston and Jorgen's proposition who argued that **15** to **30** interviews were sufficient to arrive at data saturation (Preston & Jorgen, 2016). The interviews were conducted in two universities as already extensively indicated. The universities were coded with **University A** and **University B** respectively. Table 5 illustrates the diversity of the sample population that participated in the in-depth interviews. The interviewees were enrolled based on their roles and their willingness to participate in the interviews with the initial substantive focus being given to university staff in the ICT department, faculty members, and university general staff. Every reasonable step was taken to inform the participants about the full details of the study and thereafter full consent was sought before commencing the interviews.

Table 5: Profile of interviewees with their role at the university as students, ICT, and staff

	University	Role at the University
Informant 1	University A	ICT Staff
Informant 2	University B	ICT-Staff
Informant 3	University B	ICT-Staff (Management level)
Informant 4	University A	ICT-Staff (Management level)
Informant 5	University B	ICT-Staff (Technician Level)
Informant 6	University B	ICT-Student
Informant 7	University A	ICT-Staff
Informant 8	University A	ICT staff (Technician level)
Informant 9	University A	Student
Informant 10	University A	Student
Informant 11	University B	Student (ICT)
Informant 12	University B	student (Non-ICT)
Informant 14	University B	Student (Non-ICT)
Informant 15	University A	Student (Non-ICT)
Informant 16	University A	Staff (Non-IT)
Informant 17	University B	ICT Staff (Technical Level)
Informant 18	University A	Staff (Non-Technical)
Informant 19	University B	Student
Informant 20	University B	Student

The study first started by identifying if indeed there was a *culture of information security compliance* within the two universities that were engaged. This was done by looking into the *artifacts*, *values,* and *norms* through in-depth interviews. The approach for following the *artifacts*, *values,* and *norms* was adopted from the culture model by (Schein, 1990). Evidence of information security compliance was investigated within the context of how many breaches occurred and how these breaches were mitigated over time in cases where it was reported to have occurred. Some other components of this investigation were People orientation, Ethical orientation, Adaptability, Clarity of support from senior management with regards to compliance and organizational views on excellence, and trust among its members. Once these dimensions had emerged, we identified that indeed the organizations studied had a strong sense of organizational information security compliance culture. We then worked backward to identify from the interview and field notes the factors that contributed to the information security policy culture by starting with open coding and following the Gasson, (2004) grounded theory sequence of theory generation. The results also showed strong support for *demography* as a factor that moderated or impacted the *individual's perceptions of information security policies* and *individual's attitudes towards information security policies*. Organizational factors such as *management support* and *management leading by example* also emerged strongly as moderating factors that shaped how organizational strategies like policy adoption and awareness creation among other strategies succeeded.

After several iterative rounds of data collection, coding, and analysis, several themes emerged which upon consolidation, were grouped into four main thematic groupings namely, ***demographic-oriented themes***, ***organizational-oriented themes***, ***individual-oriented themes,*** and ***information security compliance culture-oriented themes***. The organizational oriented themes were further sub-grouped into the ***organizational level factors*** and ***moderating factors***. The same was also done for individual-oriented themes to generate the ***individual-level factors*** and the ***factors moderating the individual-level factors***. We present an extensive response under Emerging themes and Informant mapping with cited quotes in **Appendix 8**.

Instances of Policy Violations and Evidence of the Culture of Compliance

We set to understand the level of information security maturity within the universities. The objective was to set the stage towards understanding the anticipated focus of the availability of information security culture. We asked questions that would elicit responses that would highlight how the universities in question had been dealing with breaches if at all they ever happened and how frequently they have experienced breaches. Responses suggested a form of maturity in terms of managing information security and executing the respective information security policies.

After establishing the status of breaches and level of compliance in the universities, we set out to establish the manifestation of information security compliance culture in the two universities. The responses indicated that the universities had some level of information security compliance culture. This was evident from the comments of the IT managers in the two universities who highlighted the continuous compliance actions from the members of the institutions. An example can be drawn from the ***2nd informant*** who highlighted that, "…*there is an environment with following the rules and policies within the university*…". Similarly, the ***1st and 2nd informants****'* acknowledgment of very minimal concerns of information security breaches can act as a pointer to the conclusion that indeed there is a culture of complying with information security policies.

For example, one of those interviewed talked about a few internal information security breach incidents.

> "*…Fairly speaking, we have not had major incidents of information security…*" ***1st informant***

> "*…We have not had serious cases internal or maybe someone going against the policy and probably acting against our security measures, but we have once in a while had had issues of carelessness, someone does something costly, an example is that we use a database in a different section where one is given access to develop and does an update that wipes and messes the systems due to human error but due to backup, we can always restore. Internally, we have not had cases of sabotage as such because, for example, we are careful with staff when they are leaving, the exit processes safeguard us….*" ***2nd Informant***

The responses supported the establishment of information security compliance culture coupled with the management also showing huge support. To buttress this conclusion, we draw from the ***1st informant*** who alluded to a mature information security compliance culture.

> *"…As such I can say we are satisfied that the compliance culture in our institution has grown much…."* ***1st informant***

Individual-level Antecedents (Perceived Ease of ISP Application, Perceived Risks of ISP Application, Individual Attitude)

Perceived Ease of ISP Application

One of the emerging influencers from individual perspectives was the perceptions of how easy it is to understand the information security policies in place or how the ease of application of the information security policies was perceived. The sentiments were shared by the respondents that it would make it easy for them to comply if the policies were easy to understand. Policies are designed to be followed by individuals and this, they said could lead to policy circumvention if it made their lives difficult thereby leading to some form of policy violations.

> *"...We have managed to create an environment that makes it easy for our colleagues and students to work seamlessly with ICT infrastructure and software with minimal security risks. An easy ICT platform to use creates a safer acceptance...."* ***1st informant***

Perceived Risks of ISP Application

Respondents also shared their concerns that the risks perceived to be because of interacting with information security assets and policies on their personalities, informed to some extent on how they comply with related information security policies. One emerging factor was the perceived risks as an influencer of information security compliance. For example, the ***4th and the 7th informants*** expressed the concerns that exist among their peers about the risks involved when the policies are perceived to expose them to the administration. Such sentiments were said to involve situations where it was considered that their details were being captured on every website they accessed. As such, the informants *"...were more inclined to use online firewall blockers...*", without considering the risks they were exposing the institution to external compromises.

Individual Attitude

Attitude towards the actions by the administration emerged as one other pointer to how individuals behaved. It was a general observation that students who had formed an attitude towards the administration in blocking some of the access to the internet indicated that they would likely violate the policies if given the opportunity and know-how. This was a stack difference from the more mature members who would be more inclined to understand the rationale of the blockages. According to the ***8th informant***, video games and access to blocked sites provided a ground for younger members to form a negative attitude towards the policy of fair usage in the university.

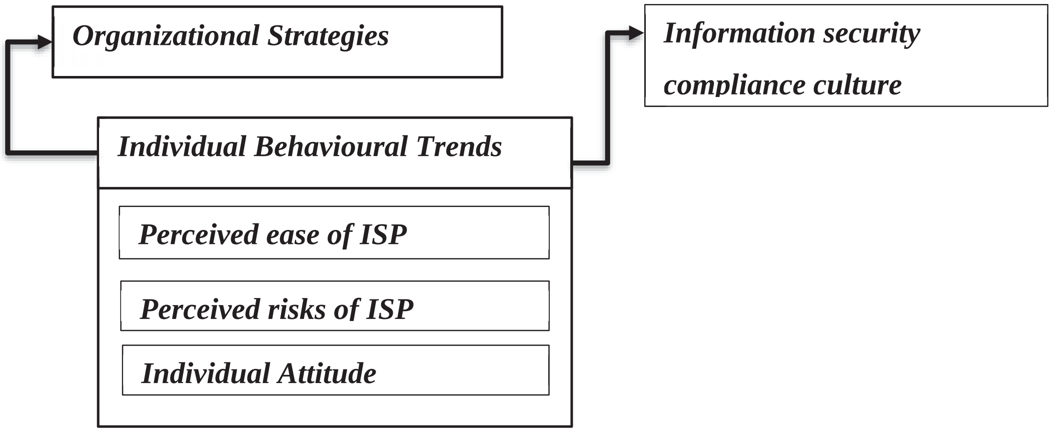

Organizational Strategies
Information security compliance culture
Individual Behavioural Trends
Perceived ease of ISP
Perceived risks of ISP
Individual Attitude

Figure 13: Influence of individual behavioral trend on organizational strategies, and information security compliance culture

Demographic Factors (Age Factor (Maturity Level), Social Upbringing, Educational Background, Educational Background)

Age Factor (Maturity Level),

From the first phase of the study, the age factor became one of the factors respondents expressed as a construct to be considered when deciding how to address information security concerns. Age was a factor in that while designing how to handle younger and senior students and staff in the universities, the generational grouping mattered in coming with an approach. For example, one respondent said that the younger generation was becoming more and more inquisitive to the point that it becomes more difficult to stop them from accessing non authorized online material despite the policies.

> *"... also one of our challenge and greatest threat, is that we have very bright students, and most of the bright students doing well outside are from here so once in a while they will try this and that but then again as I have told you based on how we give rights in the system you will have to try very hard. We have a challenge with the requests for interns and how they access our resources so even when we do grant such, we are also careful on the level of damage. So, we work on the worst-case scenario when we allocate them duties while at the same time helping them to learn. If they are given a role what is the worst, they can do...?"* ***2nd informant***

Social Upbringing

Being brought up in an environment where there was self-entitlement also emerged as one factor that management had to grapple with in most students. Coupled with the age dynamics, some students alluded to social upbringing as one factor that impacted how they perceived some policies. Some have been brought up to a more open and socialized in a society where everything and anything goes. Sharing everything online and clicking every way through social media has become part of their conscience to the extent that some of them have not grappled with the fact that such actions would expose the organizational efforts to prevent compromised situations with regards to secure sensitive content. Even efforts to keep the members safe through confidential information at times have been threatened on some occasions. This is seen in the response by the 8th informant and 9th informant who say.

> *"...I also feel that to some extent, how people are socially natured reflect on how they interact with rules and regulations. This is my opinion though. So, to some extent, I believe that it is not all of those who are in computer science who are likely to go against the rules and violate policies, some of these students are law-abiding and we have very few cases of those who are socially brought up to believe that they have the rights and freedoms to explore. We are however aware of these kinds of students and have provisioned for managing such. It is challenging but achievable…."* ***8th informant***

> *"...Social media is our lives. And that is why we have never considered it a threat to data security. Of course, there are policies of non-disclosures but whoever reads them and whoever follows them? Even if there are rules of what to share and what not to share, there needs to be a way of just filtering them rather than blocking people like us. I have some knowledge of information security but that does not mean that what I am doing by sharing can be wrong. Do you understand the group mentality? It is what mostly drives us as young people…."* ***9th informant***

Social Pressure

It emerged that there was a strong wave of influence among the young colleagues to be the hero of the peer group. To be the one who fits the *"…IT guru…"* status as indicated by the ***5th informant*** meant a big deal to some of the students. This was expressed as common among the technically oriented students. Even though there exist systems in place to monitor all actions and flag any potential compromise to the information system assets, the students have not been deterred to attempt compromising the networks especially in the quest to be the *"…one…"* with the latest pirated software.

> *"…Yes, if you interact with them you will even notice that to some extent, they teach the older generation a lot. These are people who have spent all their time on computers. The older generation only interacted with computers while working. So, there are things they wouldn't know but these young people because they spend all their time on the computer, they will know. If you interact with them from my experience, I have learned a lot from them. I would sit down, and they would tell me, you guys have blocked download of torrents, but my colleagues are still doing it, this is how they are doing it, and they show you. You get to realize that there is a backdoor. But without interacting with them you will just be wondering how comes, you go find a hard disk is full of movies, is full of books, where are they coming from. And we have blocked torrents. It is that they can identify the backdoor…"* ***5th informant***

Educational Background

Some respondents in the first phase indicated that students who were in the computer-related studies were more prone to not following the information security policy sometimes due to the nature of their studies than those in other non-computer related studies. This would be deliberate to achieve part or whole of the assignments when they needed extra software not covered by the institution. The respondents also expressed situations where the students in computer-related studies were more inclined to understand the risks but still proceed to violate the policy as opposed to those who were in non-computer related studies.

> *"…The generation we have today deals with reason and not threat. You threaten them, you encourage them to do it. You tell them these are the*

> *consequences of doing this. You bring it down to their level, especially like the ones of computer science that I am dealing with, I will tell them you are going to develop an application. How would you feel if someone posted it online for free? Now that makes them think. They put themselves in that situation and they see it wouldn't be fair to them, so why would I do it? for others? I think that is one way….”* **5th informant**

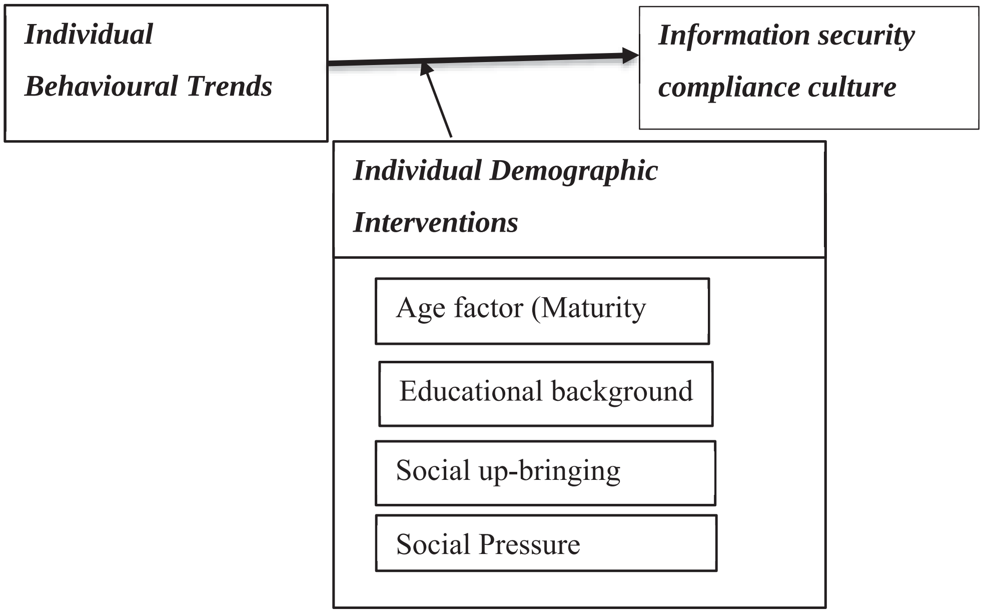

Individual Behavioural Trends
Information security compliance culture
Individual Demographic Interventions
Age factor (Maturity
Educational background
Social up-bringing
Social Pressure

Figure 14: Influence of individual demographic interventions on the relationship between individual behavioral trends and information security compliance culture

Organizational Strategies (Awareness Program, Capacity Development, Deterrence Control Mechanisms)

One of the strongest emerging themes was the factors that are related to organizational strategies. We delved deeper to understand what drove the process of ensuring the compliance culture is developed. Many informants mentioned that there was a strong awareness program by the management. There were also some sentiments on the role played by the capacity development of the members which improved a lot the incidents of policy compliance. The development of the deterrence control mechanism was also mentioned as one of the contributory factors in improved information security compliance culture.

Awareness Program

Awareness program has been documented to be one way of creating awareness culture, it was therefore not a surprise when respondents interviewed in the first phase also expressed awareness program as one of the ways of increasing information security compliance.

> *"…We have done several awareness initiatives. By this I mean that any new member of the community is given a briefing on the ICT policies in place, we have hotlines that anybody who has query can reach the IT team on….*" ***1st informant***

> *"…We have identified and even evaluated a few tools, online tools that talk about ICT security awareness and policies, so we can use a similar approach to each a wider audience because now that will be delivered right at the workstation of the user. They can do it on demand and then even measure their skills as related security…." **3rd informant***

> *"…With my many experiences in IT here in the university and elsewhere, creating awareness to your users is key many violations do not occur because of lack of policies or because people are just stubborn, but at times because they are not aware that they are violating policy. This is more so if you are handling a large group of people with deferent backgrounds…." **7th informant***

Capacity Development,

What was also expressed by the respondents as a motivator to the members to comply with information security policies, was the organizational initiative to empower their members with information and tools about the latest threats and how to handle them when they experience one. By training their members on threats emerging, the respondents responsible for securing information systems assets highlighted that this improved member's vigilance and thereby increased the possibilities of complying with information security policies.

> *"…we have not had major incidents of information security breach because we not only have a very well equipped and knowledgeable IT department who understands what needs to be done, but also a very respectable and compliant society if I may refer to staff and students alike…." **1st informant.***

> *"…The security section that deals now strictly with one of the things to enact is that they have been undertaking a lot of training on security and they are also implementing international standards in terms of the framework in security some of them look very theoretical but here when they now put in ISO as a process then they become serious because they are audited as certain parameters…."* ***2nd informant***

Deterrence Control Mechanisms

Institutional control mechanisms and processes were also expressed as one other way that contributed to the success of information security compliance. The respondents also expressed that the continuous and robust control mechanisms that were adopted in the two subject universities influenced how successful the policies were complied with. Putting in place monitoring and tracking of incidences was expressed as a way of organizational learning from the mishaps and incidents that are occurring. This was highlighted as a way of keeping history in place to help develop ways of improving. The respondents expressed that having a tracking and monitoring mechanism helped in planning for the future and shaping the lesson learned to be shared also by peer information security managers.

> *"…For you to access the examinations portal, then ICT will require you to have your MAC address, and your IP address, and then your payroll number so it is merged with this. So, if you are going home you will not be able to access it because you will be using a different machine. So, it means there is some control. If it is the results, you cannot have a pdf of it. If you need it, you will have to do the hard copy. This brings in another aspect of printing where you print from a specific [printer], it is centralized in most departments. Also, it gives some control of data…."* ***5th informant***

> *"… there [are] some controls even for the students. They cannot just access betting sites, vulgar sites because it would indicate, this is the registration number. So, I can come and say I may look for this person, it becomes easier to trace them…."* ***5th informant***

The respondents expressed the success factor in enabling information security managers to combat the issues of information security policy violations. This was done by having institutionalization of deterrence initiative for those who violate information security policies and committing information security breaches. The consciousness gained by the members concerning the punishment that will follow those who violate the policies had acted as a deterrent for the would-be violators.

> *"…Yes, we have restrictions and for example in the university even when you use the internet, you use your registration now with a password. So, it means that if you are doing anything fishy, we can be able to identify who is this. We have an ICT security who would follow up to find out, they would tell us in your lab someone trying to access this and this site. And they are doing something illegal. So, there are some controls even for the students. They cannot just access betting sites, vulgar sites because it would indicate, this is the registration number. So, I can come and say I may look for this person, it becomes easier to trace them. You will be blocked on the network such that a registration number cannot be used by any other person. And they are encouraged to be the only ones using that username and password. The username is your registration number the password you can even create your own, there is one generated by the system, but you can always create your own. So, if you give it out, it is at your own risk…." **5th informant***

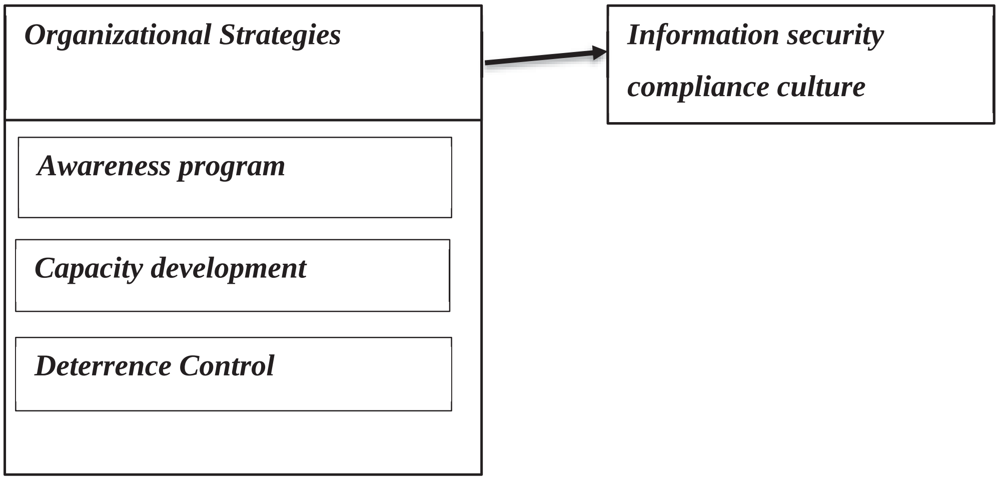

Organizational Strategies
Awareness program
Capacity development
Deterrence Control
Information security compliance culture

Figure 15: Relationship between information security compliance culture.

Management Support

Emerging also from the interviews were three other themes that relate to organizational strategies though from management perspectives. *Management support* emerged as one of the supportive pillars as identified by several informants during the interviews. We also identified a culture of management leading by example to support the information security initiative. Informants who were interviewed expressed the role played by the support. For example, *1st informant, 2nd informant, 3rd informant, and 4th informant* expressed the "*support from management*" that they have always received to enable them to function.

> *"…The management also is in full support and this gives us the best environment to succeed. We also have a population that knows what it means to do the right thing. That means that every new person joining us finds a culture of securing our information assets…"* ***1st informant***
>
> *"…Management is very keen on ICT because the way ICT works here, much as it is a department in central administration is an independent entity that is funded, and it has a budget. And part of that budget goes to NIS […Networks Infrastructure and Security…]. So, we have a budget for that. We present our budget based on the plans we have in terms of security to the management and most of the time we get the right budget to go and implement, where it is not possible, we asked for alternatives. When it is completely not possible, we go for a quick fix as we look for a permanent solution…."* ***2nd informant***
>
> *"…The support of management is actually at different levels. It starts from the ICT director here, he drives the process, then he is also in charge of updating top management periodically on policy compliance issues relating to ICT, and the top management, the way they support us is by providing, whenever we request for training related to security and any other ICT field, they support by offering/giving the facilities or the financial services that we require to go for these training…"* ***3rd informant***
>
> *"…Management supports us a lot there is a policy that has been laid out and there is usually something called standard operational procedure. Those SOPs, once the management has absorbed and accepted it, everybody [must] follows that, if it one is in breach of that, you will get the full force of that. And, even in our KPIs, revising these policies is part of it. And we always come up with a new policy as we go, and on a need basis because security is always changing. The kind of attacks that we used to get before are not the same ones…."* ***4th informant***

With regards to leadership that shows a good example by the management, the informants expressed the importance of management leading by example in conforming and respecting the laid down rules and procedures. This, according to the ***4th informant***, cascaded up to the top quarter of the senior management.

> *"…Even the VC himself does not exclusive rights to the PC. He cannot come and install anything without consulting the helpdesk. Even a Dean, cannot log in and install anything. That is how we get support. And if a dean insists that, that has to be authorized by the highest levels and they have to prove why they have to install something that is not within the university policy…."* ***4th informant***

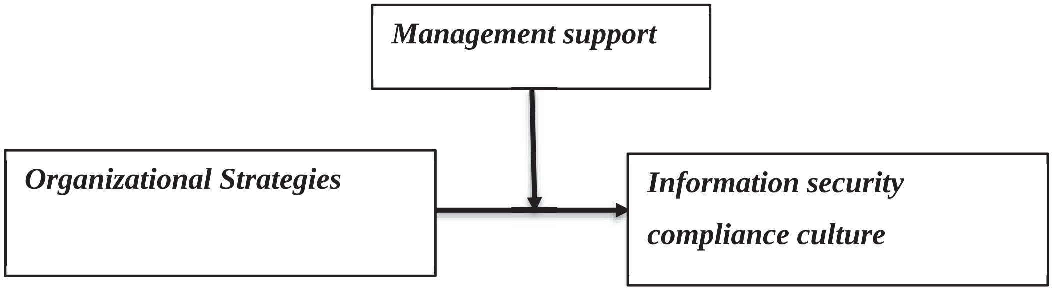

Management support
Organizational Strategies
Information security compliance culture

Figure 16: Influence of management support on the relationship between organizational strategies and information security compliance culture

Organizational External Factors (Regulatory Authorities, ISO Certification, and Standards, Best Practices from Peers)

Apart from the organizational strategies, it also emerged that there were external factors that impacted how the organizations formulated their policies as well as how they strategized to enhance policy compliance. Part of those interviewed expressed the role played *by external institutions*, standards such as *ISO certification initiatives,* and of course the *peer environment* in which they are operating.

For example, Regulatory authorities emerged as one influencer of how the university management formulated their policy and strategies regarding policy compliance. Informants suggested that the management would consider what they are bound by from the legislative and regulative perspective before they decided on a strategy as informed by *3rd informant*.

> *"…we identify a list of documents that we think would be important in impacting the process from the constitution to specific standards concerning ICT that are given by the ICT…"* ***3rd informant***

Concerning certification, it was emerging that ISO standard certification played some role in shaping how the management famulated their policies and ensure compliance. Cognizant of the underlying fact that the policies are not made in a vacuum, processes, and control need to be evident as laid out in various certification standards for one to be at the top of the pack. As such, the universities seemed to have opted to consider these standard rules as part of the basis to shape their initiatives and strategies as shown by the response from *3rd informant*.

> "…*authority and then other international standards for example ISO standards on information security and so on, then after that now we clean information from all that and then come up with a revised policy. Then the level of acceptance well we also do sensitization during and after the revision to all staff and students so the level of acceptance, well we have also surveyed to understand that so that is the level we are at*…" ***3rd informant***

Also, an emerging aspect of external factor came in the form of peer influence and best practices. The management expressed the role played by other equal institutions in the industry and outside on how best to manage information security-related issues. The learning element was expressed as key in planning and strategizing on how best to enhance the information security culture within the universities.

> *"…The methodology we use is multi-pronged, we do stakeholder involvement where we involve saying for example regulatory authorities, similar institutions, for example, other universities, then we also do benchmark with other institutions of higher learning, also outside the country, we select a few which we consider saying top universities where we want to go then we also look at the current trends as regards cybersecurity and we try then to also talk to staff and students, we can conduct surveys and interviews, there are several methods that we use, and then from that, we also do some literature review and examining…."* ***3rd informant***

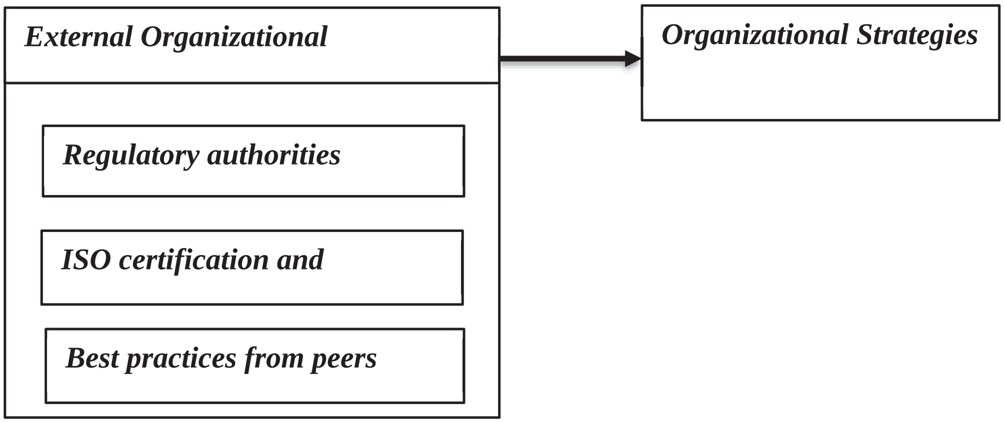


Figure 17: Relationship between external organizational interventions and organizational strategies.

4.1.1 Model Development Result Synthesis

The section shall address the research objective one which was geared towards exploring the relationship that exists between organizational culture and the information security compliance in universities in Kenya. To achieve this, we analysed the results and derived relationships encompassing the model within the context of emerging themes.

Individual-level Antecedents

Perceived Ease of ISP Application

Perceived ease of use of technology has been suggested by Workman, et al., (2008) to be an influencer towards the adoption of information security measures. This study adopted the same line of discourse to propose a relationship between perceived ease of information security policy application and information security compliance culture. This means that when it is easier to understand and apply a policy or regulation, it becomes easier to follow through with the execution of the policy in question.

This study, therefore, derives an interaction between perceived ease of information security policy application and information security compliance culture.

Perceived Risks of ISP Application

Perceptions of members in an institution that expects to succeed in the implementation of information security policies have been variously discussed in extant literature. Even though these antecedents may appear in different wording, the core message has been about the perception that those who must comply or use information systems have on the risks of the policies or information system assets. For example, Hu, et al., (2011) talks about the perceived risks of the employees violating the policies in question that they may experience because of non-compliance.

While addressing the response efficacy and self-efficacy aspect of individual behaviour's, Johnston & Warkentin, (2010) also mentions perceived threat severity as a contributor to information security compliance behavior. These ideas are also supported by (Workman, et al., 2008) who discussed the topic of perceived threat susceptibility levels as a contributor to how users respond to information security measures. Equally, Herath & Rao, (2009) points to the perceived possibility of detection as one other pointer to how users behave when they think about the possibility of being caught right in the act of violating. The same kind of narrative can be seen in the work by Sommestad & Hallberg, (2015) in which the authors discussed at length the role the threat appraisal process played in improving information security compliance intention. All these can be argued to appeal to the user inner reasoning before they act and as such, influences the general information security compliance culture. This study, therefore, derives the interactions between perceived risk of using information systems assets as having a direct relationship with information security compliance culture.

Individual Attitude

Individual attitude is one of the most studied phenomena of information security behavior if extant literature is anything to go by. Individual attitude informs behavioral trends in many ways which in turn impacts the policy compliance culture. For example, Pahnila, et al., (2007) found that the attitudes of the employees affected the general intentions to comply with information security. Similarly, Bulgurcu, et al., (2010) found that there was some influence between individual attitude and information security compliance. This seems to be the case with the findings by Ifinedo, (2014) and Safa, et al., (2016) in which both existing literature work strengthens the role played by the individual attitude in shaping the information security compliance by individuals. This study, therefore, draws a relationship between individual attitude and information security compliance culture and therefore derives an interaction between individual attitude and information security compliance culture as a direct relationship.

Individual Trend Antecedents Moderating Organizational Strategies

Organizational strategies are not made and planned in a vacuum. They must come from some form of considered influencers. Individual perceptions and individual attitudes in the said organizations are therefore a very important source of the studies. By this reasoning, this study proposes an interaction between the overall individual-level antecedents and organizational strategies towards enhanced information security compliance.

Demographic category

Age Factor (Maturity Level),

Maturity level has been found in extant literature to be a moderating factor when it comes to how individuals interact with policies. For example, Whitty, et al., (2015) found in their study that individuals at lower ages were more likely to behave in a way that would compromise information security as opposed to older and more mature persons. This kind of relationship would be considered as moderating individual-level behaviour's towards information security compliance culture.

Social Upbringing,

The way a society nature an individual has a way of informing an individual's choices and interactions. As such, borrowing from Siponen & Vance, (2010) we submit that individual shame could be moderated by how one is socially brought. This implies that social upbringing could be argued to be a moderating factor in one's behavioral interactions and intentions. Our submission also draws a similar inference from Herath & Rao, (2009) in which we argue that individual social interaction as portrayed by Herath & Rao, (2009) could have a moderating impact on an individual's behavioral tendencies. With regards to individuals' moral beliefs as portrayed by Hu, et al., (2011) it is our submission that individuals behave in a particular manner based on how they believe morally in society.

Educational Background

Literature has minimally captured the Education Background of individuals with regards to its interaction with information security compliance culture and individual actions towards it. However, we draw our argument from the close concept of Perceived Ease of technology as highlighted by (Workman, et al., 2008). It is our submission that perceived ease of technology is closely linked with education background such that those with Information Technology or computer science-related courses will have a higher understanding of information system related concepts such as information security than those who are not in the related areas of studies. As such, based on the emerging theme that depicts individuals who are in computer science-related courses as those who may understand ways of circumventing information security policies through behavioral actions, we submit that there is a moderating effect of educational background between individual's actions towards information security compliance culture.

Social Pressure

Social pressure has been discussed at length as highlighted by Herath & Rao, (2009) in which social pressure is depicted as a moderating factor in individuals' interactions with information security policies. Another pointer to the relationship that social pressure has on information security compliance was discussed by (AlKalbani, et al., 2015). Although their line of discussion was concerned with the information security culture and the actual compliance, we adopt the moderating factor concept of social pressure to the relationship between individual behavior and the information security compliance culture.

Organizational Internal Strategies

Awareness Program

Awareness programs in organizations have been linked to the success of information security management in organizations (D'Arcy, et al., 2009). The same argument is fronted by Karydaa, et al., (2005) who alluded that there is significant influence from improved awareness in organizations with regards to information security management. Similarly, Bulgurcu, et al., (2010) and Puhakainen & Siponen, (2010) support the same line of discussion by indicating that the awareness program in organizations enhances information security-conscious behavior and compliance behavior respectively. This implies that there exists a relationship between awareness programs and information security compliance culture.

Capacity Development

Improving an individual's competence through capacity development initiatives by organizations has been argued to improve information security compliance behavior. As fronted by Ifinedo, (2014) employees' competence was argued to impact how they complied with the information security policies. The same concept was seen in building employees' capabilities initiatives, which Ifinedo, (2014) also argued to be a factor in influencing information security compliant behavior. This study, therefore, adopts this line of argument by indicating a role played by capacity development to improve employees' competence and capabilities to influence information security compliance culture.

Deterrence Control Mechanisms

Organizational control mechanisms have traditionally been considered to play a role in shaping an individual's behaviour's towards information security initiatives. For example, extant literature talks about three types of control mechanisms namely preventive, detective, and corrective mechanisms (Virtue & Rainey, 2015). In applying the general deterrence theory, Chen, et al., (2014) found that deterrence controls with reward and punishments acted in a way to enhance compliance with information security policies. Penalties, according to Herath & Rao, (2009) was also considered to shape an individual's compliance behavior. This was because of fears by the individual's fear of the severity of the punishment or the risk of non-complying. Another pointer to the interaction between deterrent initiatives and information security compliance can be seen in Siponen & Vance, (2010) work in which the authors' work presented related informal sanctions to information security violations. This study, therefore, derived a relationship between deterrent control initiatives and information security compliance culture.

Organizational Internal Moderating Factors

Management Support

Top management support is a vital component in the achievement of a successful information security policy governance. Extant literature also supports this argument as can be seen in (Karydaa, et al., 2005). The authors found that participation and support from top management contributed to a successful implementation of information security policies. Availability of resources, especially when management support comes also in form of financial and budgetary allocation, has been found to impact to some extent on information security compliance strategies (Herath & Rao, 2009).

Management Leading by Example

If individual members of the organization perceive their management as leading by example, it can be argued that others will follow. Responsible leadership creates followership towards the common goal. Creating an organizational environment where leadership that leads by example creates an organizational environment that can be emulated by those being led. Organizational environment as an antecedent was proposed by Chan, et al., (2005) in which the authors found that upper management practices, direct supervision practices, and the socialization from co-workers provided a recipe for perception within an organization. It was further argued by Hu, et al., (2012) individual top management actions influenced how others in the hierarchy behaved.

Organizational External Factors

Regulatory Authorities

Coercive pressure has been found to impact management's decisions to streamline actions and strategies towards what is required at large (AlKalbani, et al., 2017). Hu, et al., (2007), further argues that coercive pressure such as those from regulatory was fronted as influencers of how organizations strategized. This study, therefore, draws a direct interaction between the regulatory authority and organizational strategies towards information security compliance culture.

ISO Certification and Standards

What is considered normal in each industry has been applied by many organizations to fit into space where others are. Normative pressure has been viewed to be one component that forces organizations to fit. With certification standards, many organizations want to be doing the right thing to fit into the "Space". This can be seen in the extant work by Hu, et al., (2007) who highlighted the role played by external normative pressure that forces managers to adopt the strategies geared towards achieving what is perceived as normal. Similar arguments are made by Cavusoglu, et al., (2015) in which the authors found normative pressure to have some influence on organizational strategies. This study, therefore, draws a direct interaction between ISO certification and standards and organizational strategies towards information security compliance culture.

Best Practices from Peers

Mimetic pressure, according to Hu, et al., (2007), has been viewed by organizational decision-makers to improve internal initiatives that follow the best of the best that is out there. Similarly, AlKalbani, et al., (2017) found that there was some influence on organizational individual strategies to follow the best practices in the industry.

4.1.2 *Putting it Together*

By summarising the whole model from the various interactions of the emerging themes, the study generates a multi-level model that explains the influencers of information security compliance culture. This was to address research objective two which was to explain the relationship that exists between organizational culture and the actual information security compliance in universities in Kenya through theory generation.

Key Variables Outcome Constructed from the Research

We synthesize the key variable outcomes by relating the analysed concept leading to the generated themes and relating the themes to the eventual dimensions. The key variables are Individual Behavioural Trends

Table 6: Systematic flow leading to the Individual Behavioural Trends key variable

Concepts	Themes	Dimensions	Key Variable
• Systems to make working with information security policies assets easy	• Improving ease of ISP application	Perceived ease of ISP application	**Individual Behavioural Trends**
• Technology acceptance initiatives that promote positive behavior	• Improving positive intentions through perceptions		
• With the ease of using ICT assets, and making ISPs accessible and easy to understand, compliance has also been on the positive trend	• Improving ISP perceptions		
• Service provision chatter, like a Service Level Agreement (SLA) within the institution • This ensures that everyone knows how and when to expect a service delivery • Ease of improving how awareness tools are implemented	• Promoting behavioral perceptions towards ICT assets and encouraging positivity		
• Trust is built over time based on the acting capacity basis in which a background check is done in the process	• Building trust among colleagues and the administration	Individual attitude	
• Some students and staff are indifferent to the administration due to suspicion that they are being watched	• Attitude towards leadership		
• There is mistrust on how the policy will affect the individual privacy	• Attitude towards policy	Perceived risks of ISP application	

Table 7: Systematic flow leading to the Individual Demographic Interventions key variable

Concepts	Themes	Dimension	Key Variable
- The nature of students in the institutions are also a factor in the information security management - systems are in place to handle this generation of young bright students	- Younger members impact on how IS management is handled	Age factor	**Individual Demographic Interventions**
- Dealing with young students on an internship within is challenging Consideration of the demography aspect in handling policy compliance-related issues	- Dealing with younger members in terms of compliance		
- Planning on the worst-case scenario while working with the young and bright interns	- Plans with the younger generation in mind		
- Lack of interest to read policies by those in the younger generation.	- Challenges in creating compliance force		
- The growing ICT trends with regards to social media has brought in more challenges with regards to information security policy management	- Challenges due to socialization context	Social pressure	
- The younger generations handling techniques important due to what society has thought them	- Societal nurturing in the wake of child rights		
- The younger generation has a way of influencing others and so investing in managing them would help create a future world of compliance	- Handling the social pressure effect		
- A structured way of tackling the generational challenges that come from them having unvetted access from a tender age	- Dealing with social upbringing	Social upbringing	
- Generational upbringing causing compliance concerns for managers due to dealing with tech-savvy and at the same time curious generation			
- The nature of the course taken can impact the rationalization of how one behaves towards policy compliance	- Education background is a factor	Educational background	

Table 8: Systematic flow leading to Organizational Strategies key variable

Concepts	Themes	Dimension	Key Variable
• Initiative to increase awareness among the members on possible threats and how to manage them • Ways to educate and create awareness initiatives among the members	• Awareness initiatives	Awareness initiatives	**Organizational Strategies**
• Prospects of awareness working to enhance compliance	• Making use of awareness to increase compliance		
• Organization initiative to manage information systems-related issues to avoid a careless breach	• Safeguards to ensure no unconscious non-compliance occur	Deterrent and Control mechanisms	
• Regulated access to only what the user needs (Control)	• Control measures		
• Least privilege access, Trust, and role-based access (Control)	• Control measures		
• Putting in place systems to reward compliance among members	• Incentives to promote compliance		
• Making it clear the consequences of non-compliance among members	• Punishments of breach actions		
• Investment in robust systems and people's capacity to handle situations to do with a potential breach	• Capacity development for the members	Capacity development	
• Involvement of the users of the policies to keep them informed on how to comply and why it is important to comply	• Capacity development to enhance conscious decision to comply		
• Training on information security as one way of enhancing information security compliance	• Capacity development to enhance conscious decision to comply		

Table 9: Systematic flow leading to the Management Support key variable

Concepts	Themes	Dimensions	Key variables
- Top management support with financing, awareness training resources, and field support, etc. Management ready to adopt SOPs and policies	- Evidence of management recognizing the role of security management	Management support	**Management Support**
- Evidence of periodic review of the information security policies by management	- Culture of taking responsibility as managers		
- Management ready to support and adopt documented incidents and policies	- Evidence of management support		
- Evidence of strategy to enhance information security policy management through KPIs	- Culture of taking responsibility as managers		
- The independence of the ICT department is guaranteed. The ICT department is well funded	- Evidence of Management taking ICT support seriously		
- A dedicated information security management structure always creates a solution to handle information security challenges	- Culture of taking responsibility as managers		
- Evidence of leading by example from the top management when they are the first to follow the rules	- Management leading by example		

Table 10: Systematic flow leading to the External Organizational Factors key variable

Concepts	Themes	Dimension	Key Variable
• ISO certification standard requirements drive part of the initiatives to review information security policies	Influence of certifications on internal decisions	ISO certification and standards	**External Organizational Factors**
• National requirements by Government also provides a reason for information security policy renewals • External regulations such as the ICT Authority and Communication Authority also influence how and when the information security policies are reviewed. • Annual auditing of the institution by external and Internal entities on conformity to the processes the institution has set aside	Influence of government pressure	Regulatory authorities	
• Borrowing from what is working from peer institutions help shape the strategies • External incidents also prompt the initiatives to review existing policies and strengthen any loopholes that may exist • Reports of impact on other institutions is a great learning point on how not to approach policy compliance	Impact of external incidents and practice on internal strategic undertakings	Best practices from peers	

We then consolidated the key variables and the dimensions as indicators to form the theoretical model as displayed in Figure 18.

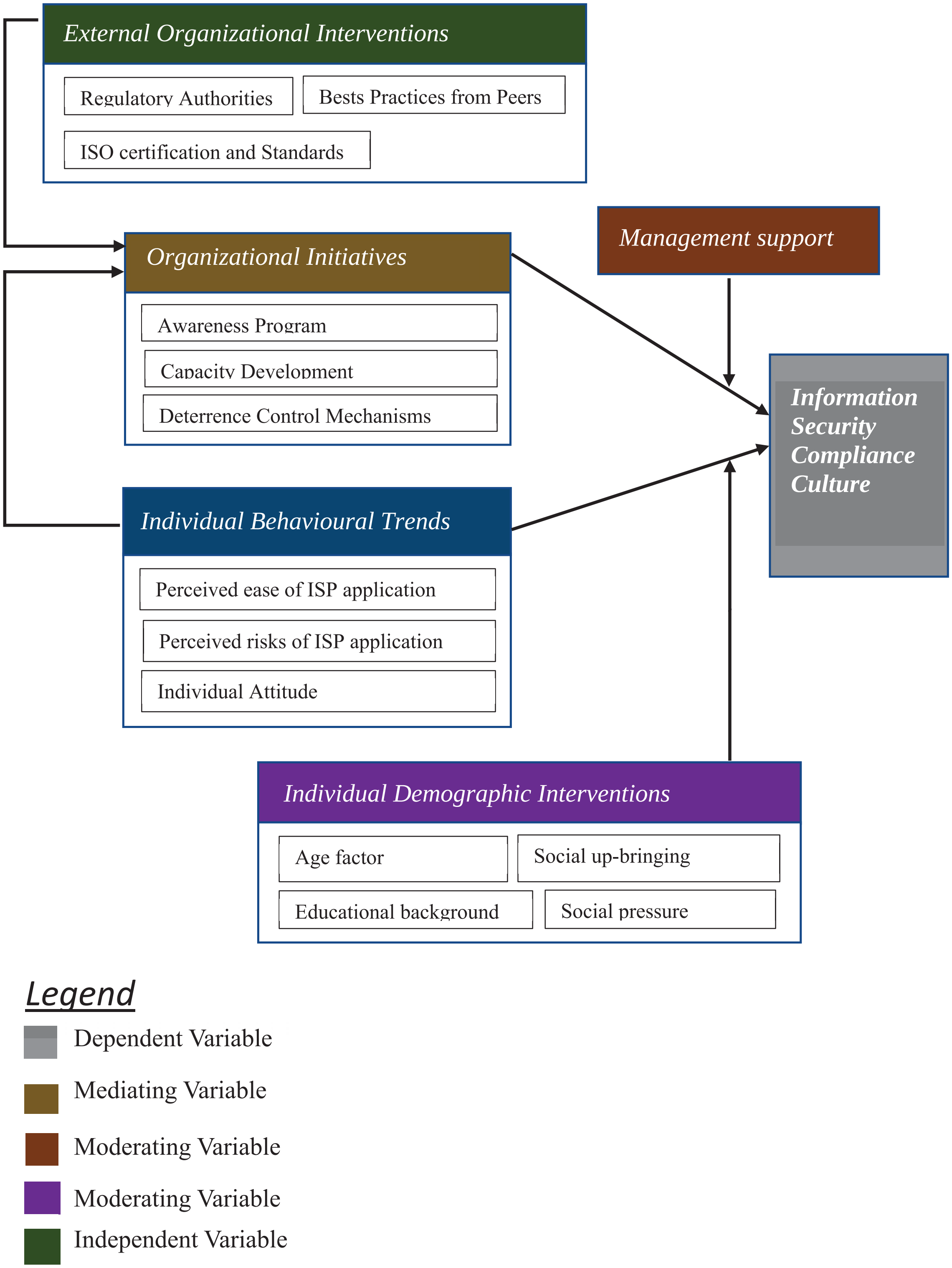

External Organizational Interventions
Regulatory Authorities
Bests Practices from Peers
ISO certification and Standards
Organizational Initiatives
Awareness Program
Capacity Development
Deterrence Control Mechanisms
Management support
Information Security Compliance Culture
Individual Behavioural Trends
Perceived ease of ISP application
Perceived risks of ISP application
Individual Attitude
Individual Demographic Interventions
Age factor
Social up-bringing
Educational background
Social pressure
Legend
Dependent Variable
Mediating Variable
Moderating Variable
Moderating Variable
Independent Variable

Figure 18: Compiled Multi-Level model for interactions between external organizational interventions, organizational strategies, individual behavioral trend, and Information security compliance culture

4.2 Model Validation Phase Results

Out of the expected 384 respondents, the study managed to receive responses from a total of 364 respondents. This translated to a 95% response rate. A detailed respondent profile is discussed in the next sections. The results are presented in three main contexts, individual demographic variables, institutional profile variables, and model validation variables. The results are highlighted based on the Demographic questions and the Confirmatory Factor Analysis context. The study tested the emerging theoretical model by applying a quantitative study through a structured questionnaire. Our findings highlighted the relevant parameters that sought to give validity to the model fit measurements such as; *Chi-square test, Additional fit measures (Comparative Fit Index (CFI), Tucker-Lewis Index (TLI), and Bentler-Bonett Non-normed Fit Index (NNFI)), Other fit measures (Root mean square error of approximation (RMSEA), Goodness of fit index (GFI)), Factor loadings, and the Model plot*. The findings also demonstrated the reliability analysis of the study via *Cronbach's α* parameter. The demographic findings and cultural artifacts are also highlighted.

4.2.1 The Demographic Findings and Cultural Artifacts Results

i. Demographic Makeup and Institutional Profile Results

The study sought to assess the demographic makeup of the respondents and the institutional artifacts, values, and norms as seen in the questionnaire in Appendix 7. The demographic makeup and institutional profile are covered in section A and section B parts of the questionnaire respectively. This aspect aimed to determine the diversity and ensure that there was substantive representation. The findings are highlighted below.

ii. Distribution of Respondents per Universities

A total of 8 universities were enrolled in this study. Out of the total respondents from all the universities enrolled, many of the respondents came from Egerton University which stood at 64 respondents. The second highest submissions came from Jomo Kenyatta University of Agriculture and Technology with submissions totalling 59 respondents followed by Strathmore University with 52 submissions. The fourth and the fifth-highest number of submissions came in from Kenyatta University with a total of 49 submissions, and Maseno University with a total of 46 submissions respectively. Substantive submissions also came in from African Nazarene University, Daystar University, and Moi University with total submissions standing at 44, 26, and 24 respondents respectively submitting responses. Table 11 summarizes the responses in percentage.

Table 11: Distribution of respondents per Universities

University	Number of respondents	Percentage of the total
African Nazarene University	44	12.1%
Daystar University	26	7.1%
Egerton University	64	17.6%
JKUAT University	59	16.2%
Kenyatta University	49	13.5%
Maseno University	46	12.6%
Moi University	24	6.9%
Strathmore University	52	14.3%
Total	364	

iii. The Gender Profile of the Respondents

The researchers sought to capture the distribution of the respondent in terms of gender. Out of the 364 respondents, the female gender was 165, and the male gender 195 of those who made the submissions. Figure 19 displays the chart in percentage with the male being 53.6%, and female submission amounting to 46.4% of the total respondents.

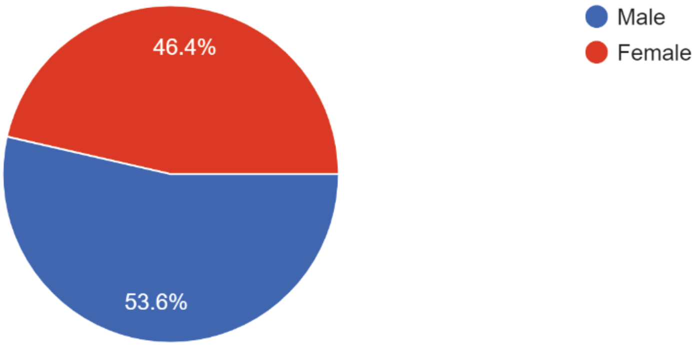


Figure 19: Respondents categorization by gender

iv. Age Group Profile of the Respondents

The researchers also sought to capture the respondents' age groups. The age groups were divided into 5 major clusters namely, Less than 20, 20 – 30, 31 – 40, 41 – 50, and Over 50. Out of those who made their submissions, none of the respondents were Less than 20 age group which stood at 0 respondents in the age group. The majority of the respondents, however, were within the 20-30 age group which was 196 submissions, this translated to 53.8% as seen in Figure 20. The age groups of 31-40 had a total of 122 submissions, this translated to 33.5% of the total respondents. The age group that ranged between 41-50 had a total of 44 respondents falling within the group, this translated to 12.1% of the respondents. The results also have the respondents over the age of 50 being only 2 respondents, this translated to 0.5% of the total respondents.

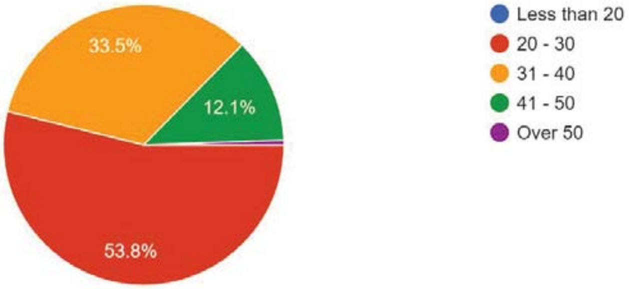


Figure 20: Respondents categorization by Age Group

v. Professional and Status of the Respondents at the University

The study also sought to capture the role of the respondents at the university in terms of whether they were students or staff. If they were staff, the study sought to understand which line of the profession they were in. The categories of staff were broadly categorized in terms of management, IT-related, and Non-IT related. Out of the 364 submissions, most of the submissions came from students, which in totality was 193 (53%). The respondents who were staff in the IT profession were 80 in total, this translated to 22% of the total submissions.

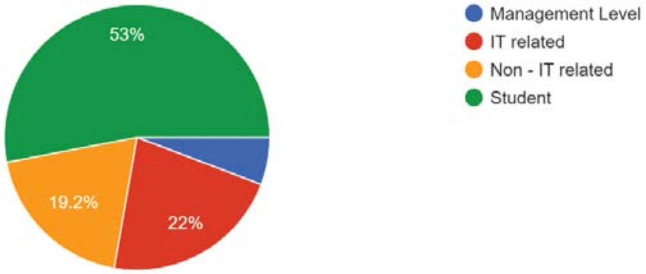


Figure 21: Respondents categorization by Occupation/Role at the University

vi. Profile of the Respondents in Terms of the Highest Level of Educational Attainment

Concerning the question about the highest level of education, Figure 22 shows the distribution of the respondents. For instance, out of the 364 submissions, Bachelor's degrees were 211 (58%), while Diploma degree accounted for 68 (18.7%) of the total. Those with a master's degree were 42 in total amounting to 11.5% while High school degrees were 22 which translated to 6% of the total. Respondents with Doctor of Philosophy on the other hand amounted to 21 respondents which translated to 5.8%. There were no respondents with a Vocational degree which stood at 0.

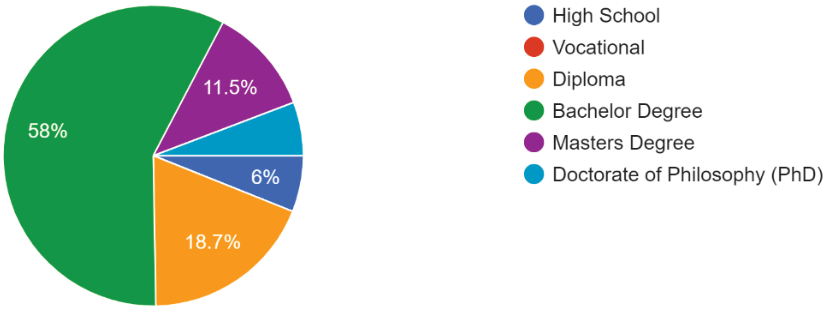


Figure 22: Respondents categorization by the Highest Education Level

vii. Profile of the Respondents by Education Background

Results on the respondent's educational background reflected IT-related education background to 169 respondents while Business management related education background amounted to 136 respondents. The respondents who had Humanity related education background were 58 in total., there were no respondents with Medicine and surgery-related education background. Only 1 respondent indicated to be from Secretarial related background.

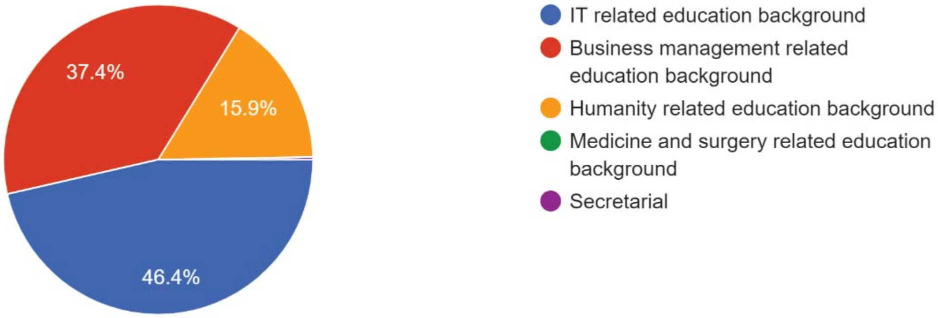


Figure 23: Respondents categorization by Education Background

viii. Does Your Institution Have Information Security Related Policy(s) in Place?

When the respondents were asked whether their universities had information security in place, a total of 299 answered in the affirmative that indeed there were information security policies in place. Only 1 respondent indicated that there is no information security in place. A total of 3 respondents also indicated that they were not willing to disclose while those who said that they did not know were 61 respondents in total.

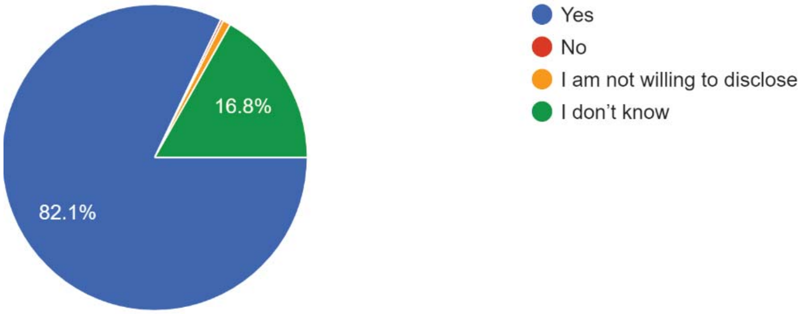


Figure 24: Responses assessing the availability of Information Security Policies

ix. Has Your Institution Ever Experienced any Information Security-related Breaches in the Last 10 Years?

The study also sought to understand how often the universities experienced information security-related breaches in the last 10 years. Out of the 364, Figure 25 shows that majority of the respondents indicated that they did not know which amounted to 208 respondents. Those who said that they have not experienced any information security breaches in the specified period were 124 respondents. Those who were not willing to disclose were a total of 25 respondents while only 7 respondents indicated that there has been some form of breaches in the last 10 years.

Out of those who had indicated a possibility of breaches, the study sought to know how the information security breaches were handles. For this question, one respondent answered, *"…There was a systematic review to address the gap that existed…"*. Another response to the follow-up question was, *"…It was a system intrusion. A new system was adapted…."*. A third answer was, *"…Limiting access to important and confidential data and capacity building student and staff on security compliance measures….". One last respondent indicated "…*Putting in place very strict regulations around information access and sharing*…."* as a way in which the breach was handled.

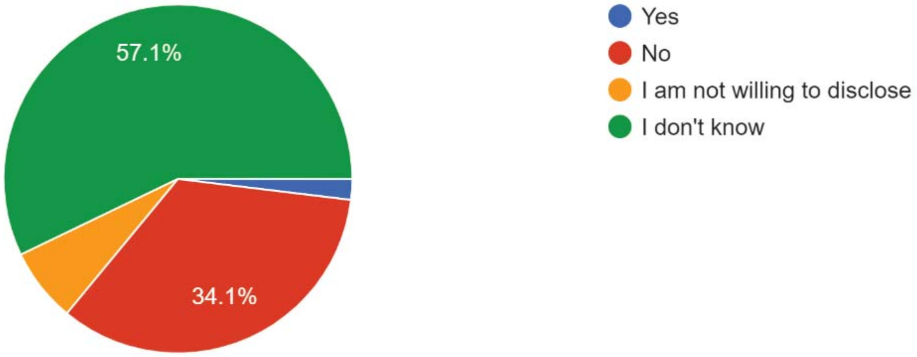


Figure 25: Responses assessing the experiences on Information Security breaches

x. How Often Does Your University Create Awareness on Information Security Policies?

On the question about awareness creation in the respective universities, many of the respondents indicated more than 5 times a year which stood at 117 submissions. A total of 113 submissions indicated that awareness activities were less than 5 times a year. Those who didn't know about awareness initiatives in their universities were 118 respondents, while those who had not seen any attempt amounted to 16 respondents.

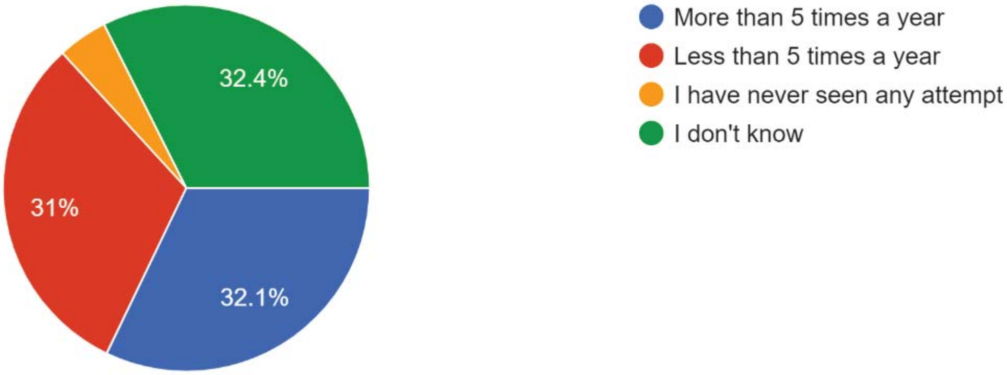


Figure 26:Responses assessing experiences with Awareness activities

xi. How Often Does Your Institution Revise Existing Information Security Policies?

In terms of how many times the individual universities revised existing information security policies, those who said the frequency was more than 5 times a year were 64 respondents. A total of 79 respondents indicated that the frequency was less than 5 times a year. Many of the respondents however indicated that they didn't know which stood at 202 respondents. Out of the total 364 respondents, 19 said they ***have*** not seen any attempt.

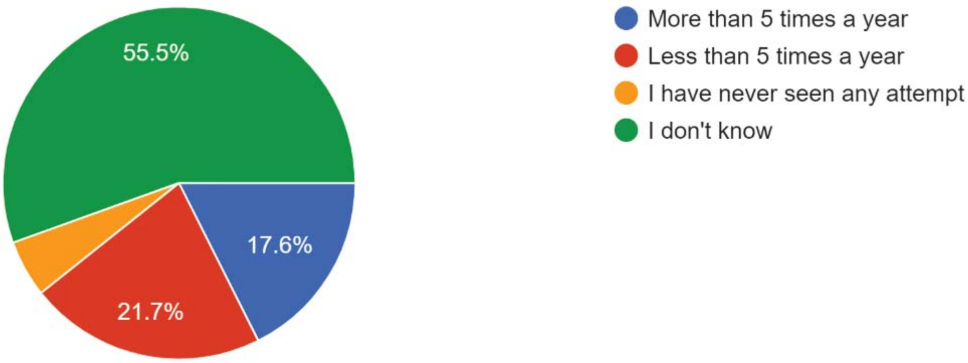


Figure 27: Responses assessing the turnover rate of Information Security policies

xii. How Often Does Your University Conduct Capacity Building Exercise on Information Security Policies and How to Handle Concerns of Information Security Breaches?

On the question about the frequencies of capacity building, a total of 98 respondents indicated more than 5 times a year while 107 indicated that capacity building initiatives were less than 5 times a year. A total of 137 respondents indicated that they didn't know while 22 indicated that there was no attempt towards capacity building.

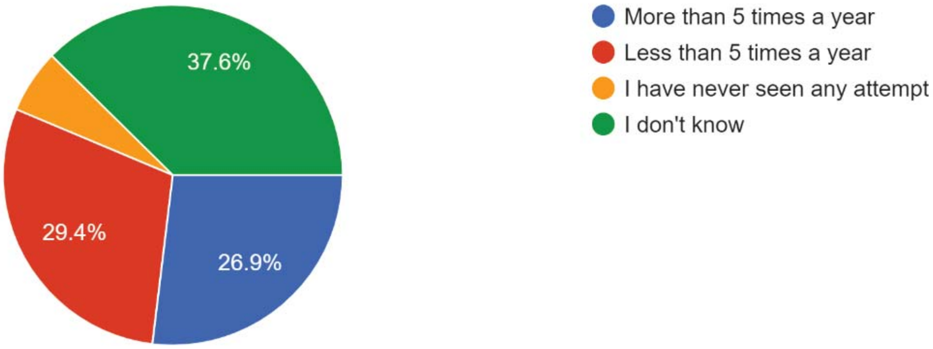


Figure 28: Responses assessing the Capacity building frequency

xiii. Do You Believe There is an Information security compliance culture in Your Institution?

A total of 255 respondents indicated that they believed there was an established information security compliance culture in their universities. A total of 13 respondents indicated that they did not believe they have an established information security compliance culture. On the other hand, 96 indicated that they did not know about any established culture of information security compliance.

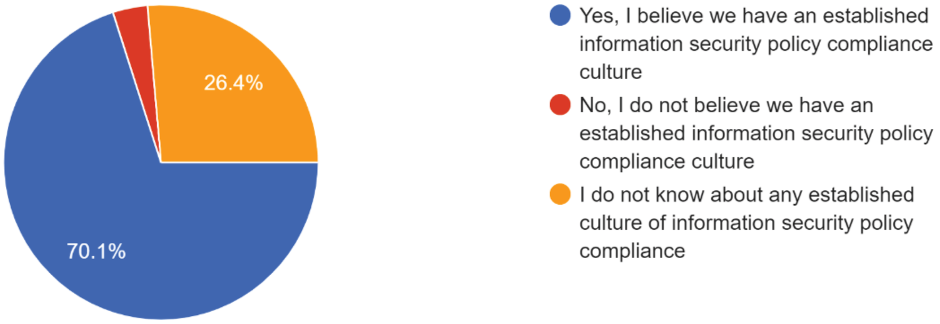


Figure 29:Responses assessing the experiences and belief in ISCC existence

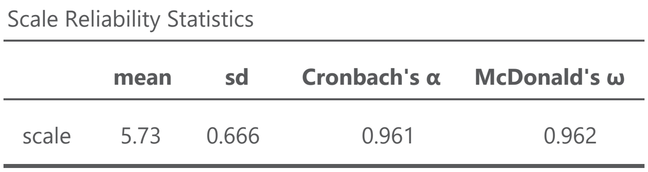
4.2.2 Model Confirmatory Factor (CFA) Analysis Validation Results

The study also validated the emerging model in section 4.4 by testing the hypothesis as summarized in section 3.5. of the confirmatory methodology phase. The questions to address this were implemented in *section C* of the questionnaire as seen in **Appendix 7**. The section adopted a seven-point Likert scale in which the respondents were to respond as either: *Strongly Agree (7), Somewhat Agree (6), Agree (5), Neither Agree nor Disagree (4), Disagree (3), Somewhat Disagree (2), or Strongly Disagree (1)*. Each scale was assigned the scaled value as indicated in their respective brackets. The findings are highlighted below.

4.2.3 Reliability Analysis

The study conducted a reliability test and the results indicate a strong result. The result is displayed in Table 12. The study applied Cronbach's α to conduct the reliability test also in Table 13 for all the variables which also show strong reliability coefficients.

Table 12: Table showing Cronbach's α value



Scale Reliability Statistics

	mean	sd	Cronbach's α	McDonald's ω
scale	5.73	0.666	0.961	0.962

Table 13: Table showing Cronbach's α value for each individual variable

Item Reliability Statistics

	if item dropped
	Cronbach's α
DMF-AF1	0.960
DMF-AF2	0.959
DMF-SU1	0.960
DMF-SP1	0.960
DMF-EB1	0.959
EOI-RA1	0.959
EOI-ISO-CS1	0.959
EOI-BP1	0.959
OMF-MS1	0.958
OMF-MS2	0.959
OMF-MS3	0.959
OS-AP1	0.959
OS-CD1	0.959
OS-DC1	0.959
OS-DC2	0.959
OS-DC3	0.959
IBT-PEIA	0.959
IBT-PRIA	0.960
IBT-IA1	0.960
IBT-IA2	0.960
OS-ISCC	0.958
IBT-ISCC	0.959

4.2.4 Model Fit

The study assessed the Chi-square test to validate the model. The result indicated a statistically highly significant value of $p < .001$. As seen in Table 14.

Table 14: Table detailing the Chi-square test

Chi-square test			
Model	**X^2**	**df**	**p**
Baseline model	6239.15	190	
Factor model	533.944	160	< .001

4.2.5 Parameter Estimates

The study also presents the factor loading for all parameters in which all the factor loadings were beyond the threshold as shown in Table 15.

Table 15: Table showing factor loading for each of the parameters

Factor Loadings					
Factor	**Indicator**	**Estimate**	**SE**	**Z**	**p**
Individual Behavioural Trends	IBT-IA2	0.655	0.0324	20.2	< .001
	IBT-IA1	0.647	0.0365	17.7	< .001
	IBT-PRIA	0.693	0.0363	19.1	< .001
	IBT-PEIA	0.664	0.0300	22.1	< .001
Organizational Strategies	OS-DC3	0.684	0.0369	18.5	< .001
	OS-DC2	0.715	0.0397	18.0	< .001
	OS-DC1	0.731	0.0393	18.6	< .001
	OS-CD1	0.624	0.0378	16.5	< .001
	OS-AP1	0.654	0.0395	16.6	< .001
Management Support	OMF-MS3	0.751	0.0409	18.4	< .001
	OMF-MS2	0.783	0.0427	18.3	< .001
	OMF-MS1	0.810	0.0387	20.9	< .001
External Organizational Interventions	EOI-BP1	0.778	0.0378	20.6	< .001
	EOI-ISO-CS1	0.862	0.0366	23.5	< .001
	EOI-RA1	0.892	0.0368	24.2	< .001
Individual Demographic Interventions	DMF-EB1	0.830	0.0421	19.7	< .001
	DMF-SP1	0.814	0.0425	19.2	< .001
	DMF-SU1	0.808	0.0471	17.1	< .001
	DMF-AF2	0.849	0.0439	19.3	< .001
	DMF-AF1	0.740	0.0472	15.7	< .001
Dependent Variable (ISCC)	OS-ISCC	0.600	0.0355	16.9	< .001
	IBT-ISCC	0.595	0.0313	19.0	< .001

4.2.6 Model Plot

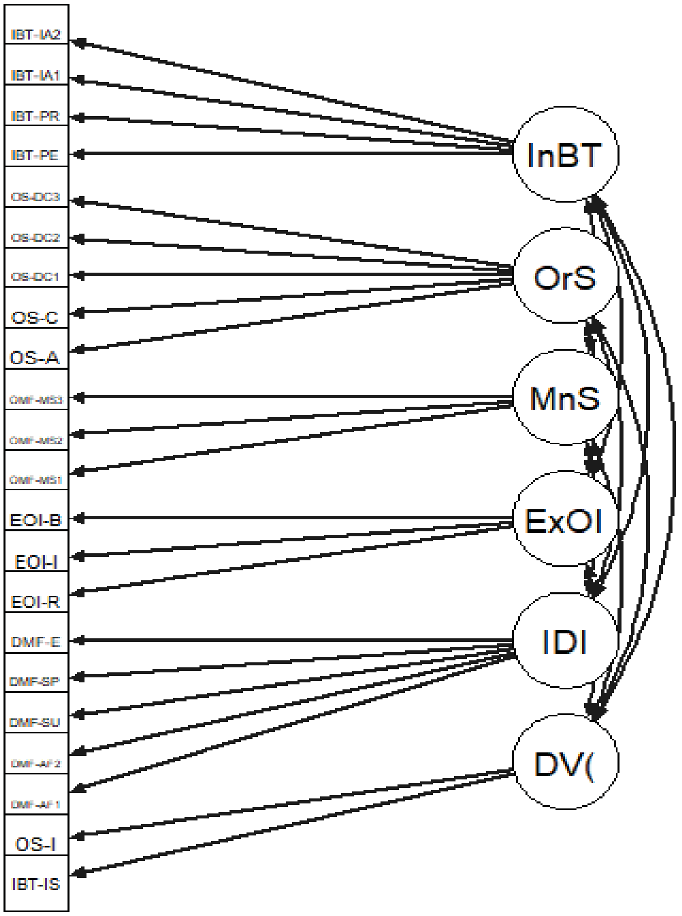


Figure 30: Model plot showing coefficients for the confirmatory factor analysis

4.2.7 Moderation Analysis

Moderation analysis was conducted to determine the moderation effects of Management Support on Organizational Strategies and the ISCC outcome. The same was also conducted to determine the moderation effect of Individual Demographic Interventions on Individual Behavioural Trends and ISCC outcome. The illustrations of the moderating effects are presented in Figure 31 and Figure 32 below. Figure 31 presents the moderating illustration of Management Support on the effect of Organizational Strategies on the ISCC. Figure 32 presents the moderating illustration of Individual Demographic Interventions on the effect of Individual Behavioural Trends on the ISCC.

The coefficients showed significant moderation effects which were all above the threshold of $p<0.005$. The P-value for the management support moderation effect was $p<0.05$ with a z coefficient value of (-1.95). This moderation effect is also demonstrated clearly in figure 33 which displays a point of convergence between low values and higher values of management support upon organization strategies. In principle, if there is no significant moderation effect, the graph should appear in parallel. This is contrary to the findings.

The moderation test for individual Demographic Interventions also showed a significant moderation effect with p-Value being less than the threshold of 0.05. Since the p-value for Demographic Intervention showed a higher value of p<0.007, the moderation effect was accepted.

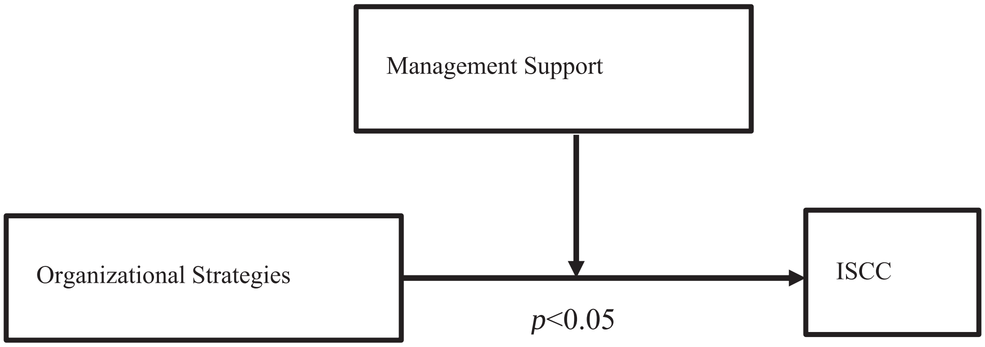


Figure 31: Illustration of the moderating effect of Management Support on Organizational Strategies and ISCC

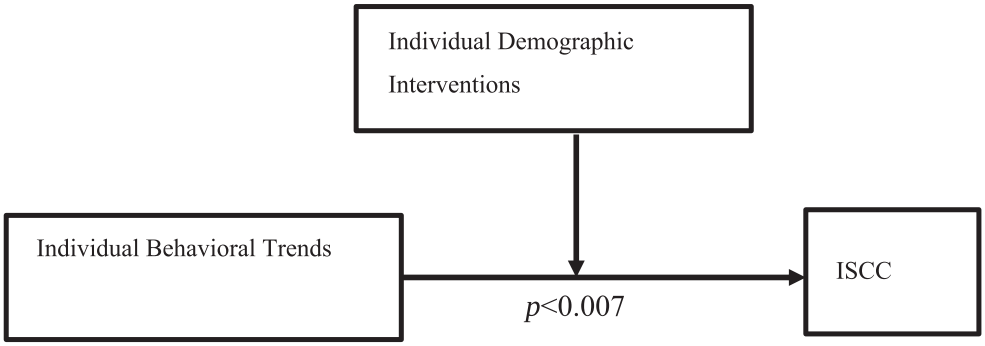

Individual Demographic Interventions
Individual Behavioral Trends
ISCC
p<0.007

Figure 32: Illustration of the moderating effect of Individual Demographic Interventions on Individual Behavioral Trends and ISCC

Table 16: Moderation estimated for Management Support variable

	Estimate	SE	Z	p
OI-ToT	0.4779	0.0164	29.07	< .001
MS-MoD	0.2834	0.0136	20.87	< .001
OI-ToT ✻ MS-MoD	-0.0207	0.0106	-1.95	0.05

Table 17: Simple slope estimates showing interactions of the moderating variable

	Estimate	SE	Z	p
Average	0.478	0.0165	29.0	< .001
Low (-1SD)	0.496	0.0149	33.4	< .001
High (+1SD)	0.459	0.0224	20.5	< .001

*Note. S*hows the effect of the predictor (OI-ToT) on the dependent variable (ISCC) at different levels of the moderator (MS-MoD)

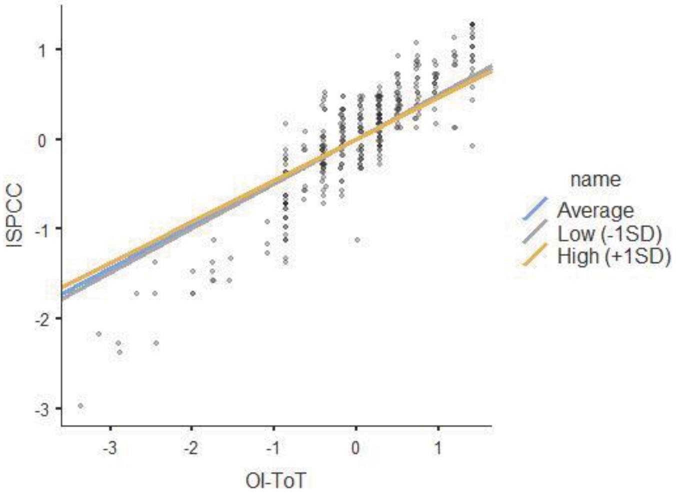


Figure 33: Graphical representation illustrating the interaction effect of Management Support on Organizational Strategy and ISCC

Table 18: Moderation estimated for Individual Demographic Intervention variable

	Estimate	SE	Z	p
IBT-ToT	0.3493	0.0136	25.75	< .001
IDI-MoD	0.4848	0.0131	37.11	< .001
IBT-ToT ✻ IDI-MoD	-0.0302	0.0113	-2.69	0.007

Table 19: Simple slope estimates showing interactions of the moderating variable

			95% Confidence Interval			
	Estimate	**SE**	**Lower**	**Upper**	**Z**	**p**
Average	0.349	0.0136	0.323	0.376	25.6	< .001
Low (-1SD)	0.375	0.0135	0.348	0.401	27.7	< .001
High (+1SD)	0.324	0.0193	0.286	0.361	16.8	< .001

*Note. S*hows the effect of the predictor (IBT-ToT) on the dependent variable (ISCC) at different levels of the moderator (IDI-MoD)

4.2.1 Additional Fit Measures

The study also presents findings for other fit measures to elaborate on the fit indices, information criteria, and other fit measures. The results indicate the Comparative Fit Index (CFI) as 0.938 and Tucker-Lewis Index (TLI) 0.927 as shown in, Table 20. With regards to information criteria as shown in Table 16, the results indicated Log-likelihood as -6740.580. The study also assessed other fit measures whose details can be found in Table 17. The finding shows the Root mean square error of approximation (RMSEA) as 0.080 and the Goodness of fit index (GFI) as 0.983. The results also show a Cronbach's α test with strong reliability of 0.956, Table 12.

Table 20: Table detailing the Fit indices results

Fit indices			
Index		**Value**	
Comparative Fit Index (CFI)		0.938	
Tucker-Lewis Index (TLI)		0.927	
Bentler-Bonett Non-normed Fit Index (NNFI)		0.927	
Bentler-Bonett Normed Fit Index (NFI)		0.914	
Parsimony Normed Fit Index (PNFI)		0.770	
Bollen's Relative Fit Index (RFI)		0.898	
Bollen's Incremental Fit Index (IFI)		0.938	
Relative Noncentrality Index (RNI)		0.938	

Table 21: Table detailing the Information criteria

Information criteria			
		Value	
Log-likelihood		-6740.580	
Number of free parameters		70.000	
Akaike (AIC)		13621.160	
Bayesian (BIC)		13893.961	
Sample-size adjusted Bayesian (SSABIC)		13671.880	

Table 22: Table highlighting other fit measures

Other fit measures			
Metric		**Value**	
Root mean square error of approximation (RMSEA)		0.080	
RMSEA 90% CI lower bound		0.073	
RMSEA 90% CI upper bound		0.088	
RMSEA p-value		7.320e -11	
Standardized root mean square residual (SRMR)		0.045	
Hoelter's critical N (α = .05)		130.879	
Hoelter's critical N (α = .01)		140.432	
Goodness of fit index (GFI)		0.983	
McDonald fit index (MFI)		0.598	
Expected cross-validation index (ECVI)		1.851	

4.2.2 Simple Slope Plot

A two-way interaction test was done that show the effect of Individual Behaviour trends on ISCC when the Individual Demographic Intervention moderation variable was factored in. The findings show that Individual Demographic Intervention has a moderation effect as seen in the interactions in the graph.

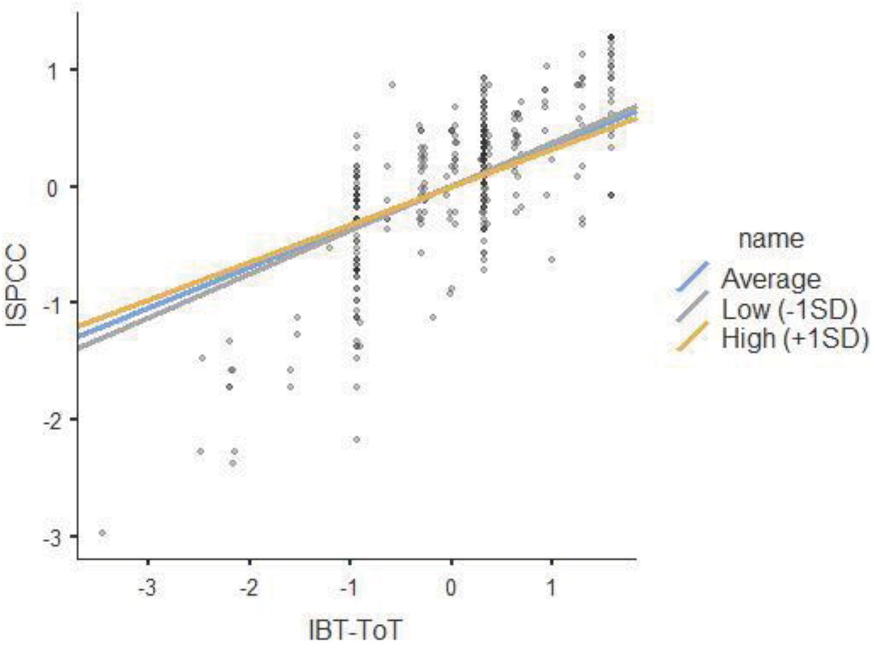


Figure 34: Graphical representation illustrating the interaction effect of Individual Demographic on Individual Behavioural Trends and ISCC

4.2.3 Mediation Analysis

We conducted three-level tests for mediation analysis. The levels were Indirect effect, Direct effect, and Total effect. The illustrations are depicted below.

The findings show the indirect effect through organizational strategies to be higher as compared to a direct effect of external organizational interventions. The total effect is also much higher as compared to the direct effect. In terms of the percentage mediation (100%), the total effect is observed in the indirect path between external organizational interventions and ISCC through organizational strategies. This shows the mediation characteristics of organizational strategies.

The p-values for the mediation coefficients were all significantly identified at p<0.001. This implies the mediation effect of Organizational Initiatives between External Initiatives. This research concludes that there was a significant mediation effect of Organizational Initiatives since the total effect was observed to show a strong mediation coefficient estimates at *c=0.576* as opposed to the direct effect *c'=0.0138*.

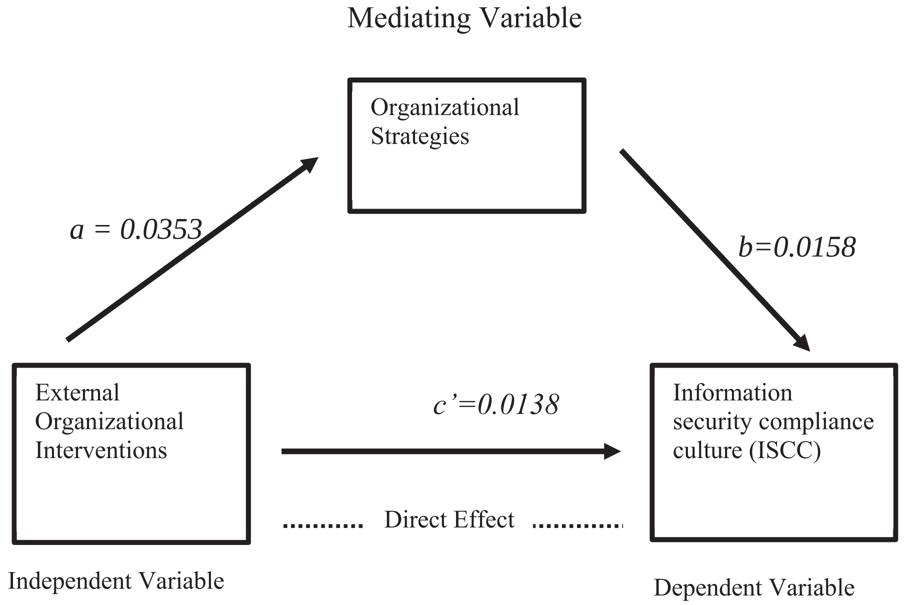

Mediating Variable
Organizational Strategies
a = 0.0353
b=0.0158
External Organizational Interventions
c'=0.0138
Information security compliance culture (ISCC)
Direct Effect
Independent Variable
Dependent Variable

Figure 35: Mediation paths for Independent and Dependent variables

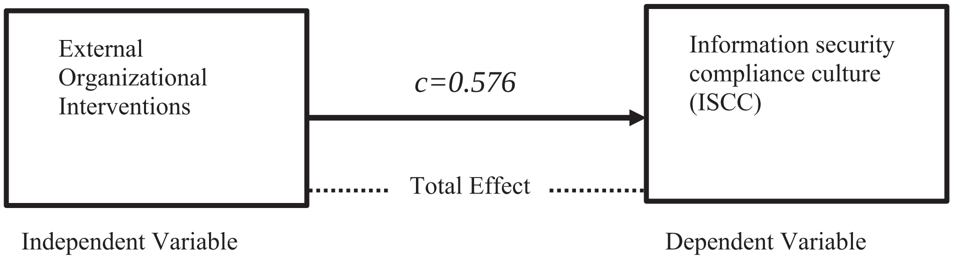

External Organizational Interventions
c=0.576
Information security compliance culture (ISCC)
Total Effect
Independent Variable
Dependent Variable

Figure 36: Total effect for the independent variable and dependent variable through the mediation variable

The findings also showed an indirect effect through organizational strategies to be higher as compared to a direct effect of individual behavior trends when tested directly. The total effect is also much higher as compared to the direct effect. In terms of the percentage mediation (100%), the total effect is observed in the indirect path between individual behavioral trends and ISCC through organizational strategies. This shows the mediation characteristics of organizational strategies.

As seen in figure 37 and Figure 38, this research concludes that there was a significant mediation effect of Organizational Initiatives since the total effect was observed to show a strong mediation coefficient estimates at *c=0.6* as opposed to the direct effect *c'=0.277*.

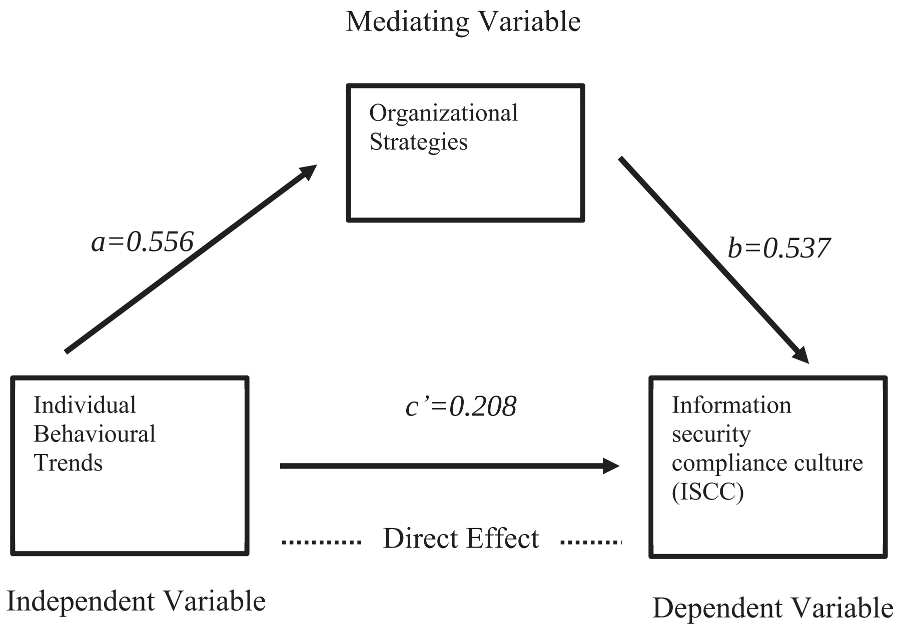

Mediating Variable
Organizational Strategies
a=0.556
b=0.537
Individual Behavioural Trends
c'=0.208
Information security compliance culture (ISCC)
Direct Effect
Independent Variable
Dependent Variable

Figure 37: Mediation paths for Independent and Dependent variables

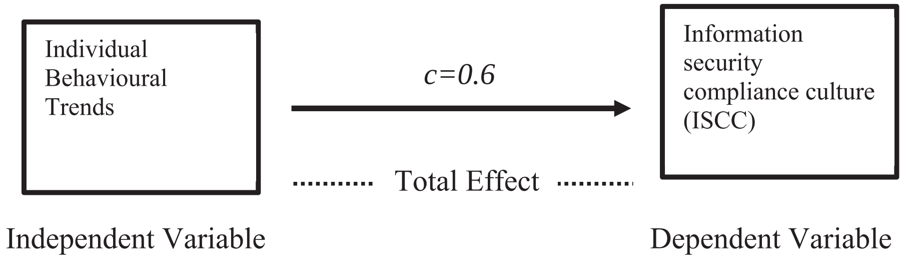

Individual Behavioural Trends
c=0.6
Information security compliance culture (ISCC)
Total Effect
Independent Variable
Dependent Variable

Figure 38: Total effect for the independent variable and dependent variable through the mediation variable

Organizational Initiative Mediation Estimates Between External Organization Interventions and ISCC

Table 23: Mediation coefficients of Organizational Initiative Between External Organization Interventions and ISCC

Effect	Label	Estimate	SE	Z	p	% Mediation
Indirect	a × b	0.299	0.0209	14.3	< .001	51.9
Direct	c	0.277	0.0138	20.1	< .001	48.1
Total	c + a × b	0.576	0.0218	26.5	< .001	100.0

4.2.4 Path Estimates

Table 24: Illustration of the path estimates showing direct, indirect, and direct values for the Mediation

			Label	Estimate	SE	Z	p
EOI-ToT	→	OI-ToT	a	0.556	0.0353	15.7	< .001
OI-ToT	→	ISCC	b	0.537	0.0158	34.1	< .001
EOI-ToT	→	ISCC	c	0.277	0.0138	20.1	< .001

4.2.5 Estimate Plot

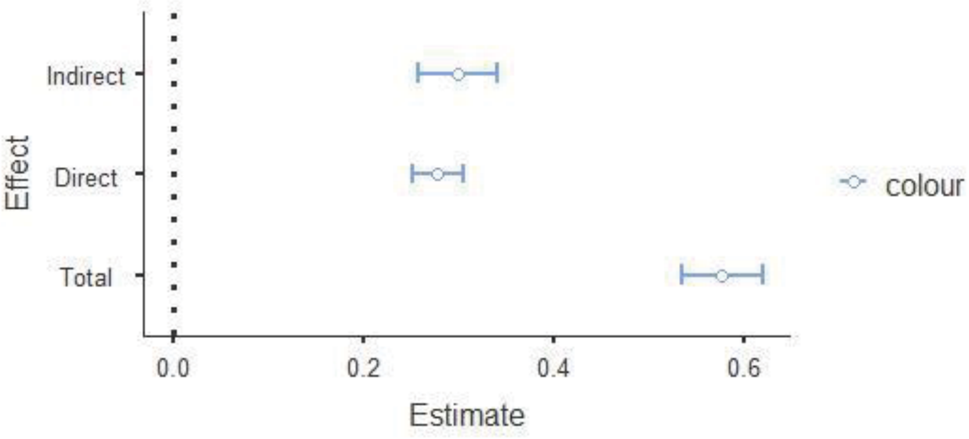


Figure 39: Estimation of the mediation effect of Organizational Initiatives

4.2.6 Organizational Initiatives Mediation Estimates Between Individual Behaviour Trends and ISCC

Table 25: Mediation coefficients of Organizational Initiatives Between Individual Behaviour Trends and ISCC

Effect	Label	Estimate	SE	Z	p	% Mediation
Indirect	a × b	0.392	0.0252	15.56	< .001	65.3
Direct	c	0.208	0.0211	9.85	< .001	34.7
Total	c + a × b	0.600	0.0250	24.00	< .001	100.0

4.2.7 Path Estimates

Table 26: Illustration of the path estimates showing direct, indirect, and direct values for the Mediation

			Label	Estimate	SE	Z	p
IBT-ToT	→	OI-ToT	a	0.673	0.0346	19.45	< .001
OI-ToT	→	ISCC	b	0.582	0.0224	25.95	< .001
IBT-ToT	→	ISCC	c	0.208	0.0211	9.85	< .001

4.2.8 Estimate Plot

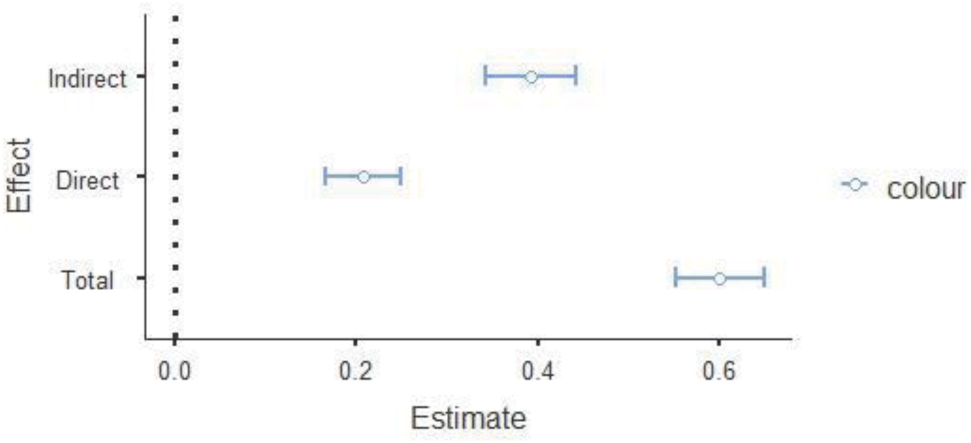


Figure 40: Estimation of the mediation effect of Organizational Initiatives

4.2.9 Model Validation Phase Analysis

We have generated a theoretical model in phase one of this study and validated the model in phase two of the study. In this section, the findings are discussed concerning the phase two objectives of the study; comparative models in existence; theoretical underpinnings; relevance to practice; and relevance to academics.

The scope of phase two of the study was only to validate the theoretical model that was generated in phase one of the study. The study had adopted the QUAL+Quan strategy of conducting a mixed method by (Peng, et al., 2011). The QUAL+Quan methodological approach is discussed in *section 3* of this thesis. This means that the study's emphasis was more on the qualitative phase because it addressed two objectives, while the quantitative phase addressing only one objective.

4.2.10 Hypothesis test outcome

Table 27: A summary outcome of the hypothesis and whether they were proved or not proved in the confirmatory validation phase.

Hypothesis	**Test outcome (Proved/Not proved)**
H1: Age has a moderating effect between *Individual Demographic Interventions* and *information security compliance culture*.	Proven
H2: Social upbringing to some extent influenced how users complied with information security policies	Proven
H3: Social pressure has a moderating effect between *Individual Demographic Interventions* and *information security compliance culture*.	Proven
H4: Education background influences information security compliance	Proven
H5: Management support has a moderating effect between *Organisational External Interventions* and *information security compliance culture*.	Proven
H6: Regulatory authorities influence organizational initiatives towards information security compliance	Proven
H7: ISO certification and standards influence organizational initiatives towards information security compliance	Proven
H8: Best practices from peers influence organizational initiatives towards information security compliance	Proven
H9: Awareness program initiative by organizations influences the compliance with information security policies	Proven
H10: Capacity development initiatives by organizations influence information security culture	Proven
H11: The deterrent control initiatives by organizations influences information security compliance culture	Proven
H12: Perceived ease of ISP application influences the information security compliance culture in organizations	Proven
H13: Perceived risks of ISP application influences information security compliance culture in organizations	Proven
H14: Individual attitude influences information security compliance culture	Proven

4.3 Discussion

The objective was to validate the model arising from the first phase. This objective was met by the translated strong confirmatory factor analysis findings. The results show that the theoretical model generated from the grounded theory phase was fit to be adopted. The implication of this is that there is a strong impact of organizational culture on information security compliance. This can be read in the relationships between the behavioral, organizational, and external factors and the existing strong information security compliance sub-culture in the universities. In the following sections, the researchers discuss the findings and how relevant they are to this objective. The findings are discussed under the demography of the respondents, the institutional profile, and the factors that impact information security compliance.

4.3.1 Institutional and Respondent Demographic Profiles

The study sought to explore the institutional profile and relate it with the individuals who responded. The findings show that many students and staff alike said they believed in information security culture. Out of the total respondents, it was interesting to note that despite a substantive number of respondents indicating they did not know whether there was an information security breach in the last 10 years, they still supported the existence of information security compliance.

This was the case with the question about how many times the univerisites created awareness. Many of the respondents indicated that they either felt that the awareness initiative fell below 5 times a year, or they did not know or have never seen any attempt combined. This is important because it tells us that the belief in information security compliance culture may not be driven by awareness only, but with other salient factors as well. It is worthy to note that despite the respondents indicating that they had fewer than awareness initiatives 5 times a year, the majority of those who either did not know or did not see any attempt were students. This is significant because it explains the gap that still exists when new members get into society. Are they supposed to experience awareness, or are there ways to compensate for awareness to increase information security compliance culture?

It was also important to note that despite many of the respondents indicating that they did not know how many times the universities revised the information security policies; it did not shake their total faith in information security compliance culture in their respective universities. This shows that for both students and staff, the aspect of compliance culture is more than just policy revision. The same can be said also in the kind of response on how often the universities built the capacity of their members. The majority appeared to indicate that they experienced the capacity building initiatives more at least 5 times a year. This tells us that the universities had taken bold initiatives to educate their members on issues related to information security policies. The nature of these capacity initiatives however was not within the scope of this study.

It is worth mentioning that majority of the staff were more aware of the various initiatives that the universities had than the students. This was evident in the responses regarding the universities' initiatives on information security-related policies and the incidents. This would be understandable because as a student, it would not automatic that one would know some administrative aspects of information security policies. This, however, seemed not to stop the majority to respond in the affirmative that they knew about their universities having information security policies. What this shows is that despite many of the members not having the same experiences in terms of administrative initiatives, and events, there remain some factors that made them believe that there was an information security compliance culture.

Having explored the importance of the relationship between the demography of the respondents and the institutional profile, we will now look at what the findings mean in terms of the factors that influenced the information security compliance culture. As already noted, despite a majority of the respondents at times saying they did not know about the existence of breaches in the last 10 years, or fewer indicating they did not know about the availability of awareness initiatives, there existed a strong indication that the majority believed that there were information security policies in place and that there was information security compliance culture. The question, therefore, that arose was, what was the explanation for the phenomenon? This is to be discussed under the auspices of the theoretical constructs that were validated below.

4.3.2 Individual Behavioural Trends

The Individual Behavioural Trends variable displayed a factor loading that we considered very strong as seen in Table 15. The factor loadings for the variable indicators ranged between 0.758 and 0.923 when standardized. This fell within the threshold level of 0.50. With an observed statistical significance of $p < 0.001$, the convergent validity was concluded in the affirmative. Therefore, we accepted the relationship from the theoretical model generated in Figure 18 that depicts Information security compliance culture as being influenced by Individual Behavioural Trends.

This is important because the findings show that individual behavior is an important factor when strategizing on how to enhance compliance. It shows that it is not only important to have information security policies in place, but how to factor in the net behavior of those interacting with the policy is equally important. For example, based on the findings, information security practitioners are supposed to understand how the policies will be received by their audience. This means that users will either form the will to comply if they have a notion that the policies will not complicate their lives than it is in the current form. The users also appear to worry so much about the risks of applying and following the policies. This implies that users would more likely to circumvent the policies if the perceived risks are higher. The attitude towards the leadership, the policies, and the environment in which the members are also mean a lot for the information security compliance culture.

In terms of organizational culture, this variable shows us that information security compliance can be natural if the administration of information security natures and balances the need to be strict, and the need to understand the underlying behavioral interpretations. An understanding of how the users will embrace the policies, and how to create reassurances that the policies will not harm or will be as easy to apply as possible is critical. This, in the end, will create ownership that leads to nurturing organizational level information security sub-culture. The resulting information security sub-culture will in the long term create an environment that allows a blossoming information security compliance culture for any newer member that joins the society.

4.3.3 Individual Demographic Interventions

The factor loading of the Individual Demographics Interventions variable showed a strong loading across all the indicators. We refer to Table 15 that illustrates the findings for the parameters and the factor loading values. All the factor loadings for the indicators ranged from 0.73 to 0.85 after standardization. This was statistically less than the threshold level of 0.50. All indicators were significant at $p < 0.001$ level, which indicated a convergent validity. With this result, we were able to accept the theoretical model relationship in Figure 18, which explained the impact of information security compliance culture through individual demographic interventions.

The import of this is that the validation shows some moderating influence that Individual Demographic Interventions has on the relationship between Individuals Behaviour Trends and Information security compliance culture. This, therefore, implies that managers should be cognizant of other moderating factors that could give a boost, or drag their efforts to enhance information security compliance culture. By overlooking the maturity level of the members, which may impact the overall information security culture, management may end up trying in vain to enhance policy compliance culture. It is equally important to factor in the social pressure aspect that the members may be living under. This is vital because as a manager, you would not want to craft security policy compliance in a way that leaves your systems exposed simply because you have not read well the social pressure ingredients in your institution. By taking account of possible social pressures that your audience may have, it will give you insights on how to, or how not to proceed in enforcing the policy compliance. The same can be said for social upbringing. Every society has members of different backgrounds and different understandings of how conflicts or perceptions can be handled. Therefore, if the institution has a more diverse membership with a range of social upbringing background, the management can have a better way of tailoring the information security environment to foster a culture of compliance. Different persons with different educational backgrounds have different approaches to technology-related policies. This, therefore, means that information security managers need to have different approaches that maximize the strengths and weaknesses of the members with different educational backgrounds. This is vital, especially if it would create a situation where the members feel that something should have been done differently due to their knowledge, thereby creating the potential to circumvent the laid down policies.

In terms of information security compliance culture, we argue that Individual Demographic Interventions are an important factor for the nurturing of organizational information security sub-culture. This is more evident when we relate the responses under the institutional profile and the majority who contributed towards Individual Demographic Interventions. This, therefore, supports our line of argument that information security culture provides an environment for individuals to behave rationally towards complying, and this, in turn, improves the information security compliance culture, which can then trickle down to new members and old members in the society.

4.3.4 Organizational Strategies

The factor loadings of the organizational strategies' variable showed a strong loading across all the indicators. Table 15 illustrates the findings for the parameters and the factor loading values that were recorded. All the factor loadings for the indicator variables ranged from 0.746 to 0.811 with standardization. This showed a statistical threshold that is less than the level of 0.50. A significant value of $p < 0.001$ level was also recorded for all indicators showing a convergent validity. With this result, we were able to accept the theoretical model relationship in Figure 18, which explained the impact of information security compliance culture through individual organizational strategies.

The significance of this finding can be looked at from the perspective of the important role that organizational initiatives play in creating a long-lasting culture of compliance. The values, artifacts, norms, institutionalization of practice become the rallying call for new members and existing members. This implies that for these rallying calls to be engraved in the current members, initiatives of awareness, capacity building, and deterrence mechanisms initiatives need to be robust, and effective. This would in the end implore and incentivize information security compliance behavior. It is our submission that when this gets engraved to the inner conscience of the members, the management would succeed in creating a long-term information security compliance culture.

Organizational culture, therefore, becomes an important foundation that determines how the norms, artifacts, values, and nationalization of practice are transformed to support information security compliance culture. A stronger information security sub-culture will bring forth a positive and ready foundation for nature compliance among new and existing members. Information security managers, therefore, need to understand this and create these environments for its membership.

4.3.5 Management Support

The factor loading of the Management Support variable showed a strong loading across all the indicators. We refer to Table 15 that illustrates the findings for the parameters and the factor loading values. All the factor loadings for the three indicators ranged from 0.812 to 0.884 after standardization. This was statistically less than the threshold level of 0.50. All indicators were significant at $p < 0.001$ level, which indicated a convergent validity. With this result, we were able to accept the theoretical model relationship in Figure 18, which explained the moderating relationship of management support between information security compliance culture and organizational strategies.

The finding implies that for a successful strategy as devised by information security practitioners, management support is an important pillar. Though not a direct impact, it would go a long way in supporting the initiatives of the experts in the intuition. This, in the long run, contributes immensely to the greater organizational culture. It is our submission that the organizational culture would more likely percolate deeper into the environment that promotes information security compliance culture. This could be argued to be supported by the members who perceived management support to encourage them. Members also felt that they would readily comply if the top management also complied.

Tied to the role of organizational culture, it is our submission that management support would offer a strong foundation for nurturing an information security compliance culture. This, therefore, shows the impact of organizational culture in a way to influence compliance culture through management interventions.

4.3.6 External Organisational Interventions

The External Organisational Interventions variable displayed a factor loading that we considered very strong as seen in Table 15. The factor loadings for the variable indicators ranged between 0.865 and 0.952 when standardized. This fell within the threshold level of 0.50. With an observed statistical significance of $p < 0.001$, the convergent validity was concluded in the affirmative. Therefore, we accepted the relationship from the theoretical model generated in Figure 18 that depicts Organizational strategies as being influenced by External Organisational Interventions.

The findings point to the importance of external influences on information security strategies in enhancing information security compliance. The findings remind us that our universities do not exist in a vacuum. Since what the members of the universities do might have an impact on the external partners and stakeholders. Recognizing that there are standards, best practices among peers, and regulatory obligations begin the step in the right direction to improve information security compliance. If the information security managers make it a culture to be conscious of what are the obligations, then it would create a positive environment to have what has worked well that can be adopted.

Consequently, it is our submission that organizational culture that is cognisant of regulatory obligation, best practice, and standards would provide the foundation for real and effective organizational initiative. This would, in turn, create an environment for information security compliance culture to flourish.

4.3.7 Model Structure

We now discuss the structure of the emergent model. To test whether the model meets our emergent theoretical model, we ran several tests to ascertain the mediation components and the moderation components. The findings supported the theoretical model by affirming the relationships as found in the model development phase. The coefficients that are above the p-value of 0.005 for the moderation factors and significant p-values of $p<0.001$ were significant enough for the researchers to accept the strength of the theoretical model.

4.3.8 What Does the New Model Tell Us?

We elaborate on the relationships that have been identified in the previous section in terms of a theory that explains information security compliance culture. We submit that there must be a precursor that promotes an environment where the existing information security policy is complied with. Without this precursor, the managers might face a dilemma of why a good policy does not translate good information security mitigation results. The conducive environment for compliance with time breeds a culture of compliance. This might be visible in action or might not be visible as would be the case of perception. These conducive environments in turn develop into a culture of information security as a sub-culture of the greater organizational culture. With the culture already in place, it would be easy for newer members and existing members to continue with the values and norms. The generated model explains this phenomenon starting from the precursor in the form of Individual Behavioural Trends which are moderated and influenced by Individual Demographic Interventions; Organizational strategies that are influenced by External Organisational Interventions; and moderated by Management Support. The organizational initiatives are also shaped by individual behavior in the organizations in addition to external intervention. We postulate a theory for future study of information security compliance culture based on the emergent theoretical model. Figure 41 gives the resulting multi-level theory of information security compliance culture in the form of a theoretical model.

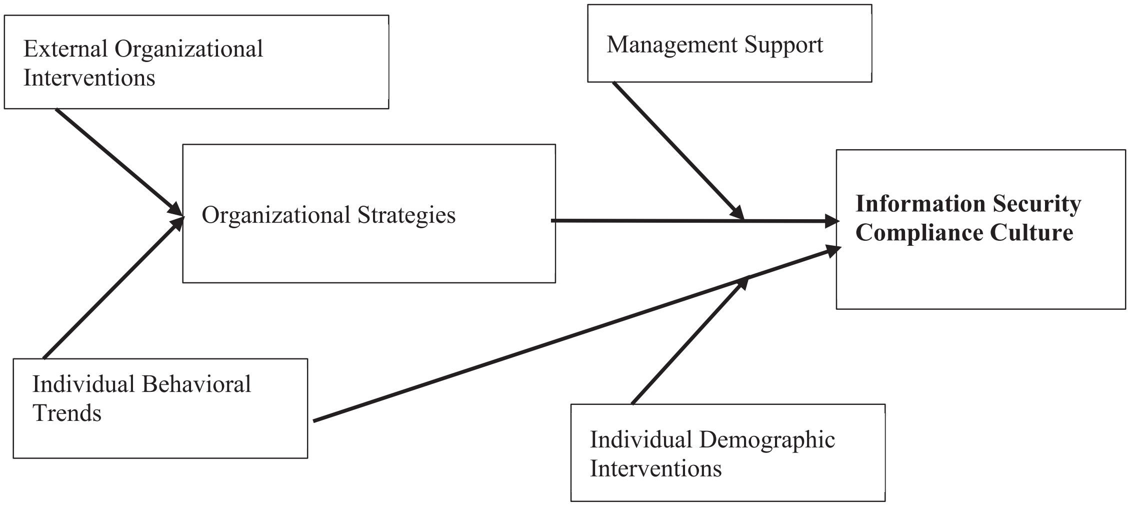

External Organizational Interventions
Management Support
Organizational Strategies
Information Security Compliance Culture
Individual Behavioral Trends
Individual Demographic Interventions

Figure 41: Top-level theoretical model depicting the relationships between Individual Behavioural Trends, Individual Demographic Interventions, Organizational Strategies, External Organisational Interventions, Management Support, and Information security compliance culture

4.3.9 How Does it Relate to Other Closer studies?

Several models have been published that attempt to theoretically explain the information security culture. However, little attention has been given to the organizational level investigation and the role of the impact of organizational culture on information security compliance. Many existing studies have applied the traditional theories in their studies such as Protection Motivation Theory, Theory of Planned Behaviour, Deterrence Theories, Institutional Theory, and Organizational Theory among others to explain the phenomena of Information security compliance culture.

This study builds up on the ongoing methodological and practical debate alongside other information security related literature by attempting to generate a theory that provides a set of propositions towards understanding information security compliance culture while allowing constructs to emerge. This is achieved by setting and presenting a systematic view of information security compliance culture. The theory, therefore, provides a solution for future information security areas of research by providing a broad variable base for future studies to explore. Existing theoretical models have focused more on either modelling on compliant behavior and policy compliance intentions. For example, models by Bulgurcu, et al., (2010), Hu, et al., (2012), and Haeussinger & Kranz, (2013) all focused on behavioral intentions to comply but little of information security compliance culture. This could be argued to be the same as the model by Chan, et al., (2014) in which the resulting model focused mainly on compliant behavior. Our model attempts to expand the scope of information security compliance study by contextualizing constructs to explain information security compliance culture.

The study Ifinedo, (2014) applied an empirical approach that considered socialization influence and cognition. This was studied through the "*Deterrence theory*" lenses. Key findings showed social bonds formed at work influenced attitudes towards compliance and subjective norms. The two constructs also emerged as having positive effects on ISSP compliance efforts by employees. The study, however, fell short to address the components of compliance culture which our study argued to be key towards long-term ISSP compliance. The utilization of existing theory to draw antecedent also did not give room to other equally important constructs to be considered. Our study adopted the grounded theory approach to let the free discovery of new constructs to build its theoretical antecedents that can explain the compliance culture elements that were not clear in the study by (Ifinedo, 2014).

The study by Tang, et al., (2015) addressed information security culture concerning organizational culture. Their focus of the study was geared towards looking at how organizational culture impacted information security compliance. The authors drew from Hofstede's organizational culture framework to generate the dimensions that were tested. Their study findings demonstrated how organizational culture impacts ISC. Their study went ahead to shows the suitability of organizational culture theories such as Hofstede's framework in offering explanations of the relationship between organizational culture and ISC. One knowledge gap that was identified was via their recommendations for future researchers to consider deployment of research in two directions. This was to possibly validate the measure for ISC and to develop exploratory models for empirical tests targeting the impact of organizational culture on ISC. Secondly, the acknowledgment of possible additional dimensions that could have been considered for their proposed ISC framework of this study exposed the antecedents' gap. Our study, therefore, took the cue of the existential gap by choosing to conduct a mixed-method, one to generate dimensions grounded on data discovery and the second one meant to validate the emerging theoretical model from data discovery. This enabled an array of constructs to emerge freely to build a theoretical model grounded on explorative data through grounded theory, and thereafter validated through a quantitative approach.

This study by Safa, et al., (2016) applied hypothesis testing to generate a model for information security compliance in organizations. Through the application of the "*Social Bond Theory*", the study proceeded to investigate the roles played by aspects of involvement as prescribed by the "*Social Bond Theory*". Their findings showed that Involving members of the organization positively influenced how they complied with information security police. The study also identified that commitment by members led to a positive influence on information security compliance. Further, the study findings showed that there was a positive influence on information security compliance through personal norms positively. The study, however, failed to delve deeper into how these constructs relate to information security compliance culture. The limitation of the singular application of one theoretical perspective also meant that there could still be more antecedents out there that could give more explanations towards information security compliance culture**.** It is from this premise that our study sought to investigate these antecedents as discovered through the grounded theory model development phase. Our study found that management support and individual behavior such as attitude shaped how information security compliance culture matured.

Another study that we analysed to identify the knowledge/theoretical gap was the study by (AlKalbani, et al., 2017). The authors approached their study from the hypothesis testing point of view to look at the role institutional pressure plays on information security compliance.

Their findings showed that information security compliance motivated the management to increase their commitment towards effort for information security compliance. Their study made great contributions towards relating institutional pressure to information security compliance. However, the approach of using singular antecedent to test left other potential constructs that could not be identified due to the prior approach. The study also did not consider the cultural aspect of compliance with information security policies. Our study opted to handle this gap by adopting a methodological approach geared towards the discovery of antecedents and theoretical development that will form a basis of information security compliance culture study. Our approach enabled the discovery process that generated showed that institutional pressure formed, to some extent, the decision-making process of ensuring compliance with information security policies.

Another study of interest was that of Amankwa, et al., (2018) in which the authors factored in variables from the involvement theory and organizational behavior theory to develop their hypothesis. Their study found that factors such as supportive organizational culture and end-user involvement significantly influenced employees' attitudes towards compliance with ISP. The overall results showed that employees' attitudes and behavioral intentions towards ISP compliance together influenced the establishment of ISCC for ISP compliance in organizations. Their study fell short of going deeper to in identification of components of information security compliance culture. This was attributed to the use of extant theories rather than exploring and generating new theoretical perspectives. Our study explored the respective elements of information security compliance culture as a sub-culture within the organizational culture. The Grounded Theory approach enabled the discovery of newer and more in-depth variables that can explain ISCC for ISP compliance in organizations. We managed to identify that supportive management and individual demographic intervention such as maturity level, educational background, social upbringing, and peer pressures influenced the general impact towards information security compliance culture.

We also benchmarked our work with the work of Sommestad, et al., (2019) in which the authors considered variables emerging from meta-analysis information security behavior tests. The meta-analysis based its antecedents on the "Theory of Planned Behaviour". Their key findings showed how the individual's anticipated regret and individual's habit improved the predictions on information security behavior. Their study, however, overlooked other aspects of information security behavior whether as predictors or as a net effect and how these elements could lead to information security compliance culture**.** It is from this premise that this study sought to go beyond the approach and employ grounded theory in a bid to discover more elements, and thereafter explain the relationships via a theory generation. As already outlined in the emergent themes, our approach managed to let indicators and thematic categories emerge.

4.3.10 What is New and Why is it Important?

To answer the question of what is new, we look at our contributions within the context of the theoretical constructs. Our theoretical model provides an expanded horizon of constructs by holistically looking at organizational, individual, and external influence to explain information security compliance culture phenomena.

To answer the question of why this is important, our theory will provide a platform for future researchers to have a starting point when studying information security compliance culture phenomena. This would reduce the struggles researchers around information security go through to borrow theories and models from other disciplines, a situation that at times does not end well for many.

4.3.11 The Relevance of the Theoretical Model?

We foresee our theoretical model to be applied practically in studies that cover information security studies. The generated theoretical model supports future studies that want to explore compliance concerning organizations, individuals, and external factors about compliance culture.

In terms of practice, the theoretical model is relevant in that it provides practitioners with a broader platform to generate a checklist for enhancing compliance culture. Studies have shown that demographic interventions and external factors have minimally been covered or if covered, have largely been very separately engaged. Our theoretical model consolidates these important variables into one thereby offering a holistic model for adoption.

In terms of academic relevance, the theoretical model offers a possibility of expansion and further refinement. Scholars would be able to explore various angles of the generated model to provide an even stronger theoretical model that explains information security compliance culture.

5.0 CONCLUSION AND RECOMMENDATIONS

In this chapter, we give a summary of the study and conclude by presenting how the research has achieved its objectives with regards to the model development explorative and model validation phases, and thereafter present the policy brief together with the limitations and recommendations.

Our study was meant to contribute towards understanding the relationships that exist between the information security culture, which is a subset of organizational culture, and the factors within universities that impact information security compliance. The expectation was to generate a theory that explains the impact of organizational culture on information security compliance culture. The research design for the study was exploratory sequential design. We adopted mixed methods in attempting to achieve this. The mixed method adopted was a mix of qualitative and quantitative methodology. In the first phase under the qualitative method, we adopted the grounded theory research design to explore and explain the emerging relationships through a theoretical model. In the second phase, we adopted a survey approach through a structured questionnaire to test and validate the model that emerged in the model development phase. By adopting this mixed-method approach, deeper comprehension of the factors that impact information security compliance culture was achieved. By applying a mixed-method, and a pragmatic philosophical underpinning, we successfully explored factors that contribute to information security compliance culture. We also successfully validated the theoretical model to confirm our newly generated theory.

In the next section 5.1, we begin with a recap of the research. This is done by highlighting key elements in each chapter. The contributions that this research has made are then discussed in the preceding section 5.2 of this chapter. We present brief policy recommendations from the research in section 5.3. of this chapter. Then we finalize with research limitations and further research opportunities in section 5.4.

5.1. A Recap of the Research

In chapter 1, we endeavoured to give a contextual background of this study and introduced the concepts of organizational culture. We also briefly discussed the concepts of information security compliance and then elaborated on our problem statements. We identified the gaps such as *little or lack of known extant studies offering knowledge on organizational culture*, *little adoption of mixed methods around information security studies*, and *lack of enough grounded theory methodologies*. In this chapter, we also set out one broad objective and three sub-objectives that will be expounded further in section 5.1.1 below.

In chapter 2, we conducted an in-depth literature review and covered the building blocks of this study in breadth while ensuring that we covered the blocks in-depth. The literature we covered explored existing works on theoretical backgrounds of organizational culture and sub-culture. We also delved deeper and explored the various paradigms of organizational culture, then followed with a concrete discussion on various organizational theories and models under organizational culture. We then explored substantively the information systems theory and related theories before finalizing the theoretical discussion with social behavioral theories. We introduced the grounded theory concept in this chapter since our grounded theory process started with an analysis of extant literature. The analysis of extant literature was meant to identify categories and themes as existing in information security compliance studies. In this chapter, we also revisited extant efforts to mitigate information security in universities such as processes and controls. We also attempted to cover extant work that investigated information security, organizational culture, and compliance to synthesize and consolidate available models that considered compliance components. The resulting consolidated outcome of the existing work was then discussed and synthesized, forming the pre-grounded theory stage by generating theoretical categories as seen in Figure 10 and Appendix 6. This chapter finalizes with an in-depth discussion of grounded theory methodology by covering the variants of grounded theory as exists in extant literature.

In chapter 3, we covered the methodology and began by discussing the philosophical underpinnings of this study. We discussed the exploratory sequential research design. We highlighted the population of the study and a diagrammatic flow of the mixed method phases. The model development phase which is an explorative study was introduced, and the model validation phase of the study was also discussed as a quantitative study. We introduced the building blocks of both qualitative and quantitative stages.

In chapter 4, we now presented the results and analysis of the explorative study as designed in the model development phase. We summarise the emergent constructs and discuss them in-depth. In this chapter, we also presented the results and analysis of the model validation phase. We also position the discussion within extant literature to draw a parallel to our study. We finalize this chapter with a theoretical model.

5.1.1 A Recap of the Research Objectives and Research Questions

We set out an overall objective to investigate and explain the relationships that exist between organizational culture and information security compliance. The rationale was to enable a theory that can be applied to explain what cultural elements are needed to enhance information security compliance alongside other initiatives like policies, processes, and controls. To achieve this broader objective, we generated three more specific objectives geared towards *Exploring the Relationship that exists between organizational culture and the actual information security compliance in universities in Kenya*; *Explaining the relationship that exists between organizational culture and the actual information security compliance in universities in Kenya through theory generation*; and *Validation of the theoretical outcome with a Quantitative approach*. The two resulting research questions from these broader objectives were, *1) What relationships exist between organizational culture and information security compliance in universities in Kenya? 2) How do these relationships impact information security compliance culture in universities in Kenya?*

The first phase of the research was more focused on the first objective and the second objective. In the explorative stage, the study achieved two key outcomes through the grounded theory approach by firstly managing to establish the information security compliance culture profiles of the university. This was followed by ascertaining the links between information security compliance and culture. A theoretical model was generated out of the constructs emerging from the explored factors. Our research successfully fulfilled its broader objective by exploring, explaining, and validating the theory. Therefore, the study answered the research question (RQ1) and research question RQ2) as follows.

The relationships between organizational culture and information security compliance in universities in Kenya?

Based on the findings of the study, organizational culture plays an important role in shaping how members comply in addition to shaping the subsequent cultural practice in the organization. However, for this cultural phenomenon to be established, the results show that there are precursors that contributes to this cultural environment of information security compliance. The organizational culture was studied within the context of the information security compliance subculture (ISCC). It was established that the universities exhibited some level of information security compliance culture (ISCC) which was supported by a strong grounding on information security policy management. The organizational culture, as exhibited through the various variables that emerged during the explorations phase supported the nurturing of ISCC.

Therefore, ISCC formed a greater organizational culture in the universities. ISCC was influenced by external organizational interventions such as regulatory authority, best practices from peers, and ISO certification and standards. These external organizational interventions impacted organizational strategies. This in effect, shaped the organizational thinking and actions towards information security compliance in the universities.

Individual behavioral trends also influenced the organizational thinking and actions towards information security compliance within the universities. Individual behavioral trends such as perceived ease of understanding information security policies (ISPs) and perceived threats of applying ISPs shaped the behavioral aspects of the members. These then shaped how the management responded towards ISP strategies in the form of organizational strategies.

The net effect of organizational strategies and individual behavioral trends impacted the environment of information security policies within the universities. This environment natured positive trends of compliance with information security policies as a culture. The internal organizational strategies played a mediation role between external organizational interventions and information security compliance while the individual behavioral trends played a direct role towards organization strategies and ISCC. This implies that internal organizational strategies played a mediating role between individual behavioral trends and ISCC.

Organizational strategies exhibited a boost from management support in the form of management leading by example. The management also supported the strategies by providing financial and administrative support to enhance the organizational initiative. This created a moderating relationship between organization strategies and information security compliance culture.

Individual behavioral trends were also moderated by individual demographic factors such as age (maturity level) of the members, social upbringing, social pressure, and educational background. These individual demographic factors partly influenced the net effect of individual behavioral trends on the individual's compliance with information security policies at the universities.

The influence of organizational culture on information security compliance culture in universities in Kenya

The organizational strategies strongly supported the formation of an information security compliance culture in the universities. Amongst the indicators tested, deterrence initiatives and awareness creation displayed a stronger impact as compared to capacity development. However, all the indicators we well within the significant threshold meaning that all the factors were accepted. This implies that when organizations have a strong organizational culture of ensuring strong deterrence and awareness initiatives, there will be a growth of information security compliance culture. Organizational initiatives such as capacity development also need to be considered because when members build their capacity, then with time they embrace the values, norms, and assumptions to grow further the ISCC.

The effect of external organizational interventions on the ISCC also showed that it was strongly mediated by organizational strategies. The regulatory authority and ISO certifications and standards emerged as the topmost parameters that were tested with standardized estimate values of over 0.9%. The regulatory authority parameter topped the list. All the parameters, however, met the acceptance thresholds to be accepted. The mediation exhibited by organizational strategies on the external organizational interventions and ISCC showed a total mediation effect of 100%. This showed that the relationship between external organizational interventions and ISCC was mediated by the organizational strategies. A similar strong mediation effect was exhibited between individual behavioral trends and ISCC. Both the mediation effects exhibited very strong mediation coefficients that allowed us to accept the relationships. This finding shows that organizations are not immune to external influence. The stricter the external regulations are, the more organizations will enforce their internal initiatives, and, in the end, this will nature ISCC.

Individual behavioral trends also impacted greatly on the ISCC. With a significant value of $p<0.001$, the individual behavioral trends showed that the direct relationship had a significant impact on the ISCC. All the tested variables that were tested showed strong values meaning that they were all included in the final model. Among the parameters that were tested, perceived ease of understanding the ISPs showed a stronger relationship than the other two namely perceived risks of applying ISPs and Individual attitudes towards the individuals. The individual attitudes, however, emerged as the second most impactful parameter followed by the perceived risks of applying ISPs. The findings show that perception of how easy it is to understand ISPs is an important factor. Members are more likely to comply with information security policy when they find it easier to comply as opposed to when the compliance requirements are complex. Similarly, members find it easier to comply when they develop positive attitudes towards the policies in place. The more positivity exhibited, the higher the compliance rates, and the more of the build-up of ISCC. The opposite can be said on the perceived threats of compliance with the policy when members chose to comply. This show that when managers do not create situations where members find the policy to be friendly, then non-compliance incident may occur.

The moderating effects of management support on the organizational strategies and the moderating effect of the individual demographic interventions also produced significant values to be accepted. With a significant $p<0.05$ value, the management support variable showed a strong moderation effect between organizational initiatives and ISCC. Similarly, with a coefficient value of $p<0.007$, there was a strong moderation effect of the individual demographic interventions between induvial behavioral tends and ISCC. This finding shows that maturity levels are important factors to consider. When handling different demographics in the universities, creating tools that speak to different levels and understanding is key. This is because the way junior members see and use information systems assets would be different from the way senior members use the same systems. This is even more challenging when handling members with different educational backgrounds, social upbringing, and different peer environments.

Organizational culture has an important role in shaping information security culture such as the policy compliance culture. However, this needs a starting point and a process of nurturing to have a level of maturity that we can now say an organization has an information security compliance culture. The theory that emerged showed that individual behaviours are important factors not to be overlooked by information security managers when strategizing on how to improve compliance with policies. The theory also pointed to the fact that internal organizational initiatives are very critical to cultivate an environment that a policy compliance culture can flourish. Equally, information security practitioners need to be conscious of the external environment since these will most definitely determine how they create strategies that can shape organizational policy compliance.

These relationships impact information security compliance culture by creating an environment where information security management would find it easier to understand the context in which they formulate the policies. By contributing to the values, norms, assumptions, and institutional artifacts in the universities, the identified relationships would shape the management's understanding of how best to strategize policy compliance component. By formulating strategies and ensuring future members also have a buy-in to the policies already in place, newer members would find it easier to conform to information security policies in the future. This would further strengthen the organizational information security compliance culture in the long run within the universities.

5.2. Research Contributions

In this section, we consolidate the research contributions within the domains of *theoretical contributions, methodological contributions, and practical contributions*. We submit that our research has delivered with regards to expectations on contributions, which is a requirement for any authoritative research work. Our major and overall contribution is attributed to the fact that, to the best of our knowledge, this is the first study that has ventured into the realms of information security compliance culture study in Kenya. Therefore, we submit that our contribution offers the backbone for future researchers who will be interested to study organizational culture and by extension, information security sub-culture in Kenyan Universities or other socio-economic sectors. Our study also opens the discourse on how we can contextualize information security culture within our National or local cultural practice to champion compliance with policies in universities. For example, one way of looking at the contribution would be to ask the question, how do our cultural backgrounds affect how we perceive compliance with information security policies? this line of question will benefit a lot from what our research has generated in terms of theoretical, methodological approaches. We further highlight the specific contributions in sections 5.2.1, 5.2.2, and 5.2.3 below.

5.2.1 Theoretical Contributions

There exists a varied understanding of what theoretical contribution is and what it is not. With this in mind, we adopted a basic understanding of theoretical contributions as outlined by (Whetten, 1989). Any study that has made a theoretical contribution needs to fit its contributions into four many building blocks namely: *what are the emergent constructs that can explain the relationships to phenomena*, *how are the constructs related to each other, and the phenomena*, *why should people care or give any consideration to the phenomena*, and *who / where / when reading together as three donate the boundary by setting limitation of the theoretical model generated*.

The emergent theory, therefore, fits this criterion because the study has proposed a theory that includes five constructs that relate to information security compliance culture namely, external organizational interventions, individual behavioral trends, organizational initiatives, management support, and individual demographic interventions.

5.2.2 Methodological Contribution

This study adopted a mixed method in achieving its objective. It is our submission that by highlighting the steps taken to achieve the objectives, we have provided a platform for future researchers also to explore the possibilities of considering the mixed-method approach.

Our study also highlights the philosophical underpinnings of the mixed-method approach. After exploring several possible philosophical schools of thought underpinning the quantitative and qualitative research, the study settled for the Pragmatic philosophy. This philosophical underpinning is a major contribution by this research because extant literature reveals few have adopted or discussed pragmatic philosophy in information systems research.

Our study also contributed methodologically by providing a systematic flow of application of grounded theory advocated by Charmaz. The study successfully employed grounded theory to generate a theoretical model and thereby contribute to theory. The study has meticulously explained its procedural approach through evidence of line by line coding in the open coding stage, as seen in **Appendix 10**, followed by an elaborate selective coding process, as seen in **Appendix 9**, and the theoretical coding process to generate a theory, as seen in **Appendix 8**. It is our submission that this study opens other methodological approaches to future studies in information systems studies, especially for future Ph.D. students. This is more so considering that information technology as a field is embracing more behavioral interactions such as machine learning, artificial intelligence, the internet of things, and many more.

5.2.3 Practical Contributions

Our study also contributes to practice. It is our submission that the emergent theoretical model will apply to information security managers who will not only develop robust policies but also have the foresight on how best to strategies on overall compliance regime. Our theoretical model provides a checklist of what information security policy management should consider when full compliance is expected. In the quest to build a culture of compliance, our study provides a locus for managers and stakeholders to nurture the organizational culture to create a *circular chain* of information security compliance culture.

5.3. Policy Recommendations

Information security in Kenya is becoming more crucial as we move towards full implementation of Vision 2030. With the expectations to take full advantage of ICT, the underlying concern of how to have watertight information security in all the transactions and endeavours becomes an imperative consideration rather than a second thought consideration. It is therefore worthy to highlight what our research considers a starting point towards policy recommendations.

- Establishing a model to have a participatory policy development process. As evident in our study, a strong and robust policy would be great for an institution, however, understanding the end-users of the policies and enabling the interaction with the users when developing the strong and robust policies would cultivate buy-in. Therefore, this study recommends policies towards models that would provide checklists for stakeholder involvement in policy formulations.
- Establish models to have frequent reviews based on social dynamics contextualizing the institutional metamorphosis. The study shows that a lot has changed in terms of keeping up with social and technological interplays. This impacts the existing policies that make it difficult to keep up with the compliance tractions. Therefore, universities

need to invest in models that oversee the changing environments and recommending the paths towards shifting the policy goals.

- Harmonize and strengthen the existing regulatory environment that considers a diverse range of challenges experienced in the management of information security compliance.
- Initiate a champion system for best practices around an information security culture that encourages information security compliance culture rather than focusing only on punishing the defaulters.

5.4. Recommendation for practice

- This work presents an opportunity for information security management to reinforce information security compliance through relooking at how the organizational culture is restructured to benefit information security management. By valuing the role culture plays in shaping behavioural dynamics in the organization, there is need for an appeal to the Vice Chancellors and all the top leadership of the universities to promote and highlight corporate culture as a precursor to information security compliance sub-culture so that information security compliance is not seen as only for a few who handle sensitive information systems assets, but for everyone who interacts with the information system assets in anyway. This is because the weakest link is the employee of user who does not know what vulnerabilities they are exposed to and how to be vigilant.

5.5. Research Limitation

Two possible limitations that may affect the generalization for this study were based on population sampling. These were the geographical limitation of the population sampling and the fact that only a few universities could participate in the initial explorative research. The geographical limitation meant that we could not reach out to other universities that were very far-flung for in-depth interviews, and as such, this could have injected a sampling error due to possible non-representation of the convenient sampling. Similarly, the exclusion of other potentially accessible universities due to selection criteria might have added to the sampling error. However, the study assumed that due to the diverse nature of the universities, by having staff and students from a diverse geographical location at any given time, the sampling error had minimal effect on the outcome of the study. This possible sampling error was cured by validating the results through covering universities in diverse geographical locations during the model validation phase.

5.6. Further Research Opportunities

Future studies can therefore consider a wider geographical coverage to minimize any possible sampling error that may occur.

We also conducted our grounded theory for a period spanning approximately two and a half months. It would be interesting to see what a longitudinal study time would yield. We recommend future studies to attempt triangulation using longitudinal studies to see how the constructs shift or remain the same. This would help strengthen the theoretical model we have developed.

We also recommend further testing of the theory in other populations to identify how the theory performs under different populations under study.

6.0 REFERENCES

Jaques, E., 1951. *The changing culture of a factory.* s.l.:s.n.

Ailon, G., 2008. Mirror, Mirror on the Wall: "Culture's Consequences" in a Value Test of Its Own Design. *Academy of Management Review,* 33(4), p. 885–904.

Ajzen, I., 1991. The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes,* 50(2), pp. 179-211.

Ajzen, I. & Fishbein, M., 1980. *Understanding Attitudes and Predicting Social Behavior.* Englewood Cliffs: Prentice-Hall.

Albright, J. J. & Park, H. M., 2009. *Confirmatory Factor Analysis Using Amos, LISREL, Mplus, and SAS/STAT CALIS,* s.l.: The University Information Technology Services (UITS) Center for Statistical and Mathematical Computing, Indiana University..

Alfawaz, S., Nelson, K. & Mohannak, K., 2010. *Information security culture: A Behaviour Compliance Conceptual Framework.* Brisbane, Australia, s.n.

AlHogail, A. & Mirza, A., 2014. *Information security culture: A definition and a literature review.* Hammamet, s.n., pp. 1 - 7.

AlHogail, A. & Mirza, A., 2015. Design and validation of information security culture framework. *Computers in Human Behavior,* Volume 49, pp. 567-575.

AlKalbani, A., Deng, H. & Kam, B., 2015. *(2015). Organisational Security Culture and Information Security Compliance for E-Government Development: The Moderating Effect of Social Pressure. PACIS.*. s.l., s.n.

AlKalbani, A., Deng, H. & Kam, B., 2015. *Investigating the Role of Socio-organizational Factors in the Information Security Compliance in Organizations.* Australia, Adelaide, s.n., pp. 1-11.

AlKalbani, A., Deng, H., Kam, B. & Zhang, X., 2016. *Investigating the Impact of Institutional Pressures on Information Security Compliance in Organizations.* Australia, Wollongong, s.n.

AlKalbani, A., Deng, H., Kam, B. & Zhang, X., 2017. Information Security Compliance in Organizations: An Institutional Perspective. *Data and Information Management,* 1(2), p. 104–114.

AlKalbani, A., Deng, H., Kam, B. & Zhang, X., 2017. Information Security Compliance in Organizations: An Institutional Perspective. *Data and Information Management,* 1(2), p. 104–114.

Allen, D., Karanasios, S. & Slavova, M., 2011. Working with Activity Theory: Context, Technology, and Information Behavior. *Journal of the American Society for Information Science and Technology,* 62(4), p. 776–788.

Al-Omari, A. et al., 2013. *Information Security Policy Compliance: An Empirical Study of Ethical Ideology.* s.l., s.n.

Alshare, K. A., Lane, P. L. & Lane, M. R., 2018. Information security policy compliance: a higher education case study. *Information & Computer Security,* 26(1), pp. 91-108.

Amankwa, E., Loock, M. & Kritzinger, E., 2018. Establishing information security policy compliance culture in organizations. *Information and Computer Security,* 26(4), pp. 420-436 .

Archer, M. et al. eds., 1998. *Critical Realism: Essential Readings.* London: Routledge.

Baker, J., 2012. The Technology–Organization–Environment Framework. *Information Systems Theory,* Volume 28, pp. 231-245.

Best, B. B., 2014. *Influencing employees' compliance behavior towards Information Security Policy,* s.l.: s.n.

Bibikas, D. & Kargioti, E., 2010. *Design Thinking: Towards a Unified View of Organizational and Technological Realms.* s.l., s.n., pp. 107-118.

Birks, D. F., Fernandez, W., Levina, N. & Nasirin, S., 2013. Grounded theory method in information systems research: its nature, diversity and opportunities. *European Journal of Information Systems (2013),* 22(1), pp. 1-8.

Blaxter, L., Hughes, C. & Tight, M., 2006. *How to Research.* 3rd ed. Buckingham: Open University Press.

Boisnier, A., 2002. *The Role of Subcultures in Agile Organizations.* s.l.:Division of Research, Harvard Business School.

Brown, T. A., 2006. *Confirmatory factor analysis for applied research.* New York: Guilford Press.

Bryant, A., 2003. A Constructive/ist Response to Glaser. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research.*

Bulgurcu, B., Cavusoglu, H. & Benbasat, I., 2010. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly,* 34(3), pp. 523-548.

Burrell, G. & Morgan, G., 1979. *Sociological Paradigms and Organisational Analysis.* London: Heinemann.

Cameron, K. S. & Quinn, R. E., 2011. *Diagnosing and Changing Organizational Culture: Based on the Competing Values Framework.* 3 ed. San Francisco, CA: Jossey-Bass.

Cameron, K. S., Quinn, R. E., DeGraff, J. & Thakor, A. V., 2007. *Competing Values Leadership: Creating Value in Organizations.* Cheltenham, UK; Northampton, MA:: Edward Elgar Publishing.

Cavusoglu, H., Cavusoglu, H., Son, J. & Benbasat, I., 2015. Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information & Management,* 52(4), pp. 385-400.

Chabrow, E., 2015. *Insider Breach Costs AT&T $25 Million.* [Online]
Available at: http://www.bankinfosecurity.com/insider-breach-costs-att-25-million-a-8089/op-1

Chang, S. E. & Lin, C. S., 2007. Exploring organizational culture for information security management. *Industrial Management & Data Systems,* pp. 1-33.

Chan, M., Woon, I. & Kankanhalli, A., 2005. Perceptions of Information Security at the Workplace: Linking Information Security Climate to Compliant Behavior. *Journal of Information Privacy and Security,* 1(3), pp. 18-41.

Chan, M., Woon, I. & Kankanhalli, A., 2014. Perceptions of Information Security at the Workplace: Linking Information Security Climate to Compliant Behavior. *Journal of Information Privacy and Security,* 1(3), pp. 18-41.

Charmaz, K., 2006. *Constructing grounded theory: A practical guide through qualitative analysis (Introducing Qualitative Methods Series).* London: SAGE Publications Ltd.

Charmaz, K., 2008. *Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis.* New Delhi: SAGE Publications Inc..

Chen, Y., Ramamurthy, K. & Wen, K., 2012. Organizations' Information Security Policy Compliance: Stick or Carrot Approach?. *Journal of Management Information Systems,* 29(3), pp. 157-188.

Chen, Y., Ramamurthy, K. & Wen, K., 2014. Organizations' Information Security Policy Compliance: Stick or Carrot Approach?. *Journal of Management Information Systems,* 29(3), pp. 157-188.

Cochran, W. G., 1977. *Sampling Techniques.* 3rd ed. s.l.:s.n.

Coleman, J. S., 1986. Social Theory, Social Research, and a Theory of Action. *The American Journal of Sociology,* 96(1), pp. 1309-1335.

Colwill, C., 2010. Human factors in information security: The insider threat - Who can you trust these days?. *Information Security Technical Report,* pp. 1-11.

Cooke, R. A. & Szumal, J. L., 2000. Using the organizational culture inventory to understand the operating cultures of organizations.. In: N. M. Ashkanasy, C. P. M. Wilderom & M. F. Peterson, eds. *Handbook of organizational culture and climate.* Thousand Oaks: Sage Publications, pp. 147-162.

Cooper, R. B. & Quinn, R. E., 1993. Implications of the competing values framework for management information systems. *Human Resource Management,* Volume 32, p. 175–201.

Corriss, L., 2010. *Information security governance: integrating security into the organizational culture.* Austin, Texas, s.n., pp. 35-41.

Crane, A. & Harris, L. C., 2002. The greening of organizational culture. *Journal of Organizational Change Management,* 15(3), pp. 214 - 234.

Creswell, J. W., 2009. *Research design: Qualitative and mixed methods approaches. :.* London: SAGE.

CSO Magazine, USSS, CERT & PWC, 2014. *2014 US State of Cybercrime Survey,* s.l.: Software Engineering Institute.

D’Arcy, J. & Herath, T., 2011. A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems,* Volume 20, p. 643–658.

D'Arcy, J., Hovav, A. & Galletta, D., 2009. User Awareness of Security Counter measures and Its Impact on Information Systems Misuse. *Information Systems Research,* 20(1), pp. 79-98.

D'Arcy, J., Hovav, A. & Galletta, D., 2009. User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research,* 20(1), pp. 79-98.

David, S., Marlys, M., David, B. & Mark, W., 2014. *A Theory of Employee Compliance with Information Security.* s.l., s.n.

Deal , T. & Kennedy, A., 1982. *Corporate Culture: The Rites and Symbols of Corporate Life, :, 1982..* Reading, MA: Addison- Wesley.

Denison, D. R. & Mishra, A. K., 1995. Toward a Theory of Organizational Culture and Effectiveness. *Organization Science,* 6(2).

DiMaggio, P. J. & Powell, W. W., 1983. The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review,* 42(2), pp. 147-160.

Dobson, P. J., 2001. The Philosophy of Critical Realism - An Opportunity for Information Systems Research. *Information Systems Frontiers,* 2(1), pp. 199-210.

Dwivedi, Y. K., 2009. *Handbook of Research on Contemporary Theoretical Models in Information Systems.* 1 ed. Hershey(PA): IGI Publishing.

Emirbayer, M. & Johnson, V., 2008. Bourdieu and organizational analysis. 37(1), p. 1–44.

Feilzer, M. Y., 2010. Doing Mixed Methods Research Pragmatically: Implications for the Rediscovery of Pragmatism as a Research Paradigm. *Journal of Mixed Methods Research,* 4(1), pp. 6-16.

Francis, J. et al., 2010. What is an adequate sample size? Operationalising data saturation for theory-based interview studies. *Psychology & Health,* 25(10), pp. 1229-1245.

Gasson, S., 2004. *Rigor in grounded theory research: An interpretive perspective on generating theory from qualitative field studies.* Hershey: PA: Idea Group.

Glaser, B. G. & Strauss, A. L., 1967. *The Discovery of Grounded Theory: Strategies for qualitative research.* New York: Aldine Publishing Company.

Goldkuhl, G., 2012. Pragmatism vs interpretivism in qualitative information systems research. *Eur J Inf Syst,* 21(2), pp. 135-146.

Gregor, S., 2006. The nature of theory in information systems. *MIS Quarterly,* 30(3), pp. 611-642.

Gregory, B. T., Harris, S. G., Armenakis, A. A. & Shook, C. L., 2009. Organizational culture and effectiveness: A study of values, attitudes, and organizational outcomes. *Journal of Business Research,* 62(7), pp. 673-679.

Gregory, K. L., 1983. Native-View Paradigms: Multiple Cultures and Culture Conflicts in Organizations. *Administrative Science Quarterly,* 28(3), pp. 359-376.

Guba, E. G. & Lincoln, Y. S., 1994. *Competing paradigms in qualitative research.* London: Sage.

Gundu, T. & Flowerday, S. V., 2013. Ignorance to Awareness: Towards an Information Security Awareness Process. *South African Institute af Electrical Engineers,* pp. 69-79.

Gupta, B., Iyer, L. S. & Aronson, J. E., 2000. A study of knowledge management practices using grounded theory approach. *Journal of Scientific & Industrial Research,* Volume 59, p. 668–672.

Haeussinger, F. J. & Kranz, J. J., 2013. *Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior.* Milan, s.n.

Herath, T. & Rao, H. R., 2009. Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness. *Decision Support Systems,* 47(2), pp. 154-165.

Herath, T. & Rao, H. R., 2009. Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness. *Decision Support Systems,* 47(2), pp. 154-165.

Herath, T. & Rao, R. H., 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems,* 18(2), pp. 106-125.

Higgins, G. E., Wilson, A. L. & Fell, B. D., 2005. An Application of Deterrence Theory to Software Piracy. *Journal of Criminal Justice and Popular Culture,* 12(3), pp. 166-184.

Hofstede, G., 1993. Cultural Constraints in Management Theories. *Academy of Management Executive,* 7(1), p. 89.

Hofstede, G., 1998. Identifying Organizational Subcultures: An Empirical Approach. *Journal of Management Studies,* 35(1), p. 1–12.

Hofstede, G., Hofstede, G. J. & Minkov, M., 2010. *Cultures and Organizations - Software of the Mind: Intercultural Cooperation and Its Importance for Survival.* s.l.:McGraw-Hill.

Homburg, C. & Pflesser, C., 2000. A multiple-layer model of market-oriented organizational culture: Measurement issues and performance outcomes. *Journal of marketing research,* 37(4), pp. 449-462.

Howe, K. R., 2012. Mixed Methods, Triangulation, and Causal Explanation. *Journal of Mixed Methods Research,* 6(2), pp. 89-96.

Hunker, J. & Probst, C. W., 2011. Insiders and insider threats—an overview of definitions and mitigation techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications,* 2(1), pp. 4-27.

Hu, Q., Dinev, T., Hart, P. & Cooke, D., 2012. Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. *Decision Sciences Journal,* 43(4).

Hu, Q., Hart, P. & Cooke, D., 2007. The role of external and internal influences on information systems security – A Neo-Institutional perspective. *Journal of Strategic Information Systems,* Volume 16, pp. 153-172.

Hu, Q., Xu, Z., Dinev, T. & Ling, H., 2011. Does Deterrence Work in Reducing Information Security Policy Abuse By Employees?. *Communications of the ACM,* 54(6), pp. 54-60.

Ifinedo, P., 2014. Information systems security policy compliance: An empirical study ofthe effects of socialisation, influence, and cognition. *Information & Management,* 51(1), p. 69–79.

Iivari, J. & Huisman, M., 2007. The relationship between organizational culture and the deployment of systems development methodologies. *MIS Quarterly,* 31(1), pp. 35-58.

Irwin, L., 2020. *54% of universities reported a data breach in the past year.* [Online] Available at: https://www.itgovernance.co.uk/blog/54-of-universities-reported-a-data-breach-in-the-past-year

Johnson , G. & Scholes, K., 1999. *Exploring Corporate Strategy.* 5 ed. Hemel Hempstead: Prentice Hall.

Johnson, G., Scholes, K. & Hallam, S., 2008. *Exploring Corporate Strategy.* 8 ed. Harlow: Pearson Education Limited.

Johnson, R. B. & Onwuegbuzie, A. J., 2004. Mixed Methods Research: A Research Paradigm Whose Time Has Come. *Educational Researcher,* 33(7), pp. 14-26.

Johnston, A. C. & Warkentin, M., 2010. Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly,* 34(3), pp. 549-566.

Jones, M. C., Cline, M. & Ryan, S., 2004. Exploring knowledge sharing in ERP implementation: An organizational culture framework. *Decision Support Systems,* 41(2006), p. 411 – 434.

Kam, H., Katerattanakul, P., Gogolin, G. & Hong, S., 2013. *Information Security Policy Compliance in Higher Education: A Neo-Iinstitutional Perspective.* s.l., s.n.

Kangas, L. M., 2009. Assessing the value of the relationship between organizational culture types and knowledge management initiatives. *Journal of Leadership Studies,* 3(1), p. 29–38.

Kankanhalli, A., Teo, H. H., Tan, B. C. & Wei, K. K., 2003. An Integrative Study of Information Systems Security Effectiveness. *International Journal of Information Management,* 23(2), pp. 139-154.

Karjalainen, M., Siponen, M. & Sarker, S., 2013. *Toward Process Theories on Employees' Compliance with IS Security Procedures: An Empirical Study.* s.l., s.n.

Karydaa, M., Kiountouzisa, E. & Kokolakis, S., 2005. Information systems security policies: a contextual perspective. *Computers & Security,* 24(3), pp. 246-260.

Kaur, K., 2016. Information Security Management of an organization with a focuson Human perspective. *International Journal of Computer Techniques,* 3(2), pp. 201-204.

Kennedy, K. C., 1983. *A Critical Appraisal of Criminal Deterrence Theory.* s.l.:Michigan State University College of Law.

Khazanchi, S., Lewis, M. W. & Boyer, K. K., 2007. Innovation-supportive culture: The impact of organizational values on process innovation. *Journal of Operations Management,* 25(4), pp. 871-884.

Kigen, P. et al., 2014. *Kenya Cyber Security Report 2014 Rethinking Cyber Security – "An Integrated Approach: Processes, Intelligence and Monitoring.",* s.l.: Serianu Ltd.

Kim, S. H., Yang, K. H. & Park, S., 2014. An Integrative Behavioral Model of Information Security Policy Compliance. *The Scientific World Journal,* pp. 1-12.

Knorst, A. M., Vanti, A. A., Andrade, R. A. E. & Johann, S. L., 2011. Aligning Information Security with the Image of the Organization and Prioritization Based on Fuzzy Logic for the Industrial Automation Sector. *Journal of Information Systems and Technology Management,* 8(3), pp. 555-580.

Kvale, S., 1994. Ten standard Objections to Qualitative Research Interviews. *Journal of Phenomenological Philosophy,* 25(2), pp. 147-173.

Lapointe, L. & Rivard, S., 2005. A Multilevel Model of Resistance to Information Technology. *MIS Quarterly,* 29(3), pp. 461-492.

Lebek, B. et al., 2013. *Employees' Information Security Awareness and Behavior: A Literature Review.* s.l., s.n., pp. 2978-2987.

Leidner, D. E. & Kayworth, T., 2006. Review: A Review of Culture in Information Systems Research: Toward a Theory of Information Technology Culture Conflict. *MIS Quarterly,* 30(2), pp. 357-399.

Lincoln, Y. S. & Guba, E. G., 1985. *Naturalistic Inquiry.* Newbury Park, CA: Sage Publications.

Lopez-Fernandez, O. & Molina-Azorin, J. F., 2011. The use of mixed methods research in the field of behavioural sciences. *Quality & Quantity,* 45(6), p. 1459.

Maarop, N. et al., 2015. Understanding Success Factors of an Information Security Management System Plan Phase Self-Implementation. *International Scholarly and Scientific Research & Innovation,* 9(3), pp. 884-889.

Martin, P. Y. & Turner, B. A., 1986. Grounded Theory and Organizational Research. *The Journal of Applied Behavioral Science,* 22(2), pp. 141-157.

Mason, M., 2010. Sample size and saturation in PhD studies using qualitative interviews. *Forum qualitative Sozialforschung/Forum: qualitative social research,* 11(3).

McSweeney, B., 2002. Hofstede's model of national cultural differences and their consequences: A triumph of faith a failure of analysis. *Human Relations,* 55(1), pp. 89 - 118.

Meyer, J. W. & Rowan, B., 1977. Institutionalized organizations: formal structure as myth and ceremony. *American Journal of Sociology,* 83(2), pp. 340-363.

Mingers, J., 2002. *Realizing Information Systems: Critical Realism as an Underpinning Philosophy for Information Systems.* s.l., s.n., p. Paper 27.

Mingers, J., Mutch, A. & Willcocks, L., 2003. Critical Realism in Information Systems Research. *MIS Quarterly,* 37(3), pp. 795-802.

Mishra, S. & Dhillon, G., 2006. *Information systems security governance research: a behavioral perspective.* New York, s.n., p. 27–35.

Moore, P. A. et al., 2011. *A Preliminary Model of Insider Theft of Intellectual Property (CMU/SEI-2011-TN-013),* s.l.: Software Engineering Institute.

Morgan, G., 1997. *Images of Organization.* Thousand Oaks, CA: Sage Publications.

Morrow, S. L., 2005. Quality and Trustworthiness in Qualitative Research in Counseling Psychology. *Journal of Counseling Psychology,* 52(2), p. 250 –260.

Muhire, B., 2012. *Employee Compliance with Information Systems Security Policy in Retail Industry. Case: Store Level Employees,* s.l.: s.n.

Mwagwabi, F., McGill, T. & Dixon, M., 2014. *Improving Compliance with Password Guidelines: How User Perceptions of Passwords and Security Threats Affect Compliance with Guidelines.* s.l., s.n., pp. 3188-3197.

Myers, M. D., 2008. *Qualitative Research in Business and Management.* s.l.:SAGE Publications.

Mykytyn, JR., P. P. & Harrison, D. A., 1993. The Application of the Theory of Reasoned Action to Senior Management and Strategic Information Systems. *Information Resources Management Journal,* 6(2), pp. 15-26.

Nabi, S. I., Asif, Z. & Mizra, A. A., 2014. When Sentry Goes Stealing: An Information Systems Security Case Study in Behavioural Context. *Acta Informatica Pragensia,* 3(3), p. 222–238.

Nahm, A. Y., Vonderembse, M. A. & Koufteros, X. A., 2004. The Impact of Organizational Culture on Time-Based Manufacturing and Performance. *Decision Sciences,* 35(4), p. 579–607.

Neuman, W. L., 2009. *Social Research Methods: Qualitative and Quantitative Approaches.* 7th ed. s.l.:Pearson.

Oates, B. J., 2005. *Researching Information Systems and Computing.* s.l.:SAGE.

oTranscribe, n.d. *oTranscribe.* [Online]
Available at: https://otranscribe.com/

Ovaska, P., 2009. *A Case Study of Systems Development in Custom IS Organizational Culture.* Boston, MA: Springer.

Pahnila, S., Siponen, M. & Mahmood, A., 2007. *Employees' Behavior towards IS Secur ity Policy Compliance.* s.l., IEEE.

Parsons, K. M. et al., 2015. The Influence of Organizational Information Security Culture on Information Security Decision Making. *Journal of Cognitive Engineering and Decision Making,* 9(2), pp. 117-129.

Peng, G. C., Nunes, M. B. & Annansingh, F., 2011. *Investigating information systems with mixed methods research.* Rome, s.n.

Preston, T. & Jorgen, S., 2016. Constraining or Enabling Green Capability Development? How Policy Uncertainty Affects Organizational Responses to Flexible Environmental Regulations. *British Journal of Management,* 28(4), pp. 649-665.

Puhakainen, P. & Siponen, M., 2010. Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly,* 34(4), pp. 757-778.

Quinn, R. E. & Rohrbaugh, J., 1983. A Spatial Model of Effectiveness Criteria: Towards a Competing Values Approach. *Management Science,* 29(3), pp. 363-377.

Rajendran, N., 2001. *Dealing With Biases In Qualitative Research: A Balancing Act For Researchers.* Kuala Lumpur, Malaysia, s.n.

Rogers, R. W., 1975. A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of Psychology: Interdisciplinary and Applied,* 91(1), pp. 93-114.

Rogers, R. W., 1983. *Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation.* New York: Guilford Press.

Roman, J., 2015. *Universities: Prime Breach Targets.* [Online]
Available at: https://www.databreachtoday.asia/universities-prime-breach-targets-a-7865

Ruppel, C. P. & Harrington, S. J., 2001. Sharing Knowledge Through Intranets: A Study of Organizational Culture and Intranet Implementation. *IEEE Transactions on Professional Communication,* 44(1), pp. 37-52.

Sackmann, S. A., 1992. Culture and Subcultures: An Analysis of Organizational Knowledge. *Administrative Science Quarterly,* 37(1), pp. 140-161.

Safa, N. S., Solms, R. V. & Furnell, S., 2016. Information security policy compliance model in organizations. *Computers & Security,* Volume 56, pp. 1-13.

Safa, N. S., Solms, R. V. & Furnell, S., 2016. Information security policy compliance model in organizations. *computers & security 56,* 56(2016), pp. 1-13.

Safriadi, Hamdat, S., Lampe, M. & Mun, M., 2016. Organizational Culture In Perspective Anthropology. *International Journal of Scientific and Research Publications (IJSRP),* 6(6), pp. 773-776.

Saunders, M., Lewis, P. & Thornhill, A., 2012. *Research Methods for Business Students.* 6th ed. s.l.:Pearson Education Limited.

Schein, E. H., 1990. Organizational Culture. *American Psychologist,* 45(2), pp. 109-119.

Schein, E. H., 1993. On dialogue, culture, and organizational learning. *Organizational Dynamics,* 22(2), pp. 40-51.

Schein, E. H., 2004. *Organizational culture and leadership.* 3 ed. San Francisco: A Wiley Imprint.

Schlienger, T. & Teufel, S., 2003. *Analyzing information security culture: increased trust by an appropriate information security culture.* Prague, Czech Republic, Czech Republic, IEEE.

Schraeder, M., Tears, R. S. & Jordan, M. H., 2005. Organizational culture in public sector organizations: Promoting change through training and leading by example. *Leadership & Organization Development Journal,* 26(6), pp. 492-502.

Schuessler, J. H. & Windsor, J. C., 2009. *General deterrence theory.* Denton, Texas: University of North Texas.

Scott, W. R., 2001. *Institutions and organizations.* 2nd ed. Thousand Oaks, CA:: Sage.

Scott, W. R. & Davis, G., 2008. *Organizations and organizing: rational, natural and open systems perspectives.* New Jersey: Prentice Hall.

Shafiu, I., Wang, W. Y. & Singh, H., 2016. Information Security Compliance Behaviour of Supply Chain Stakeholders: Influences and Differences. *International Journal of Information Systems and Supply Chain Management,* 9(1), pp. 1-16 .

Shareef, M. A., Kumar, V., Kumar, U. & Hasin, A. A., 2009. *Theory of Planned Behavior and Reasoned Action in Predicting Technology Adoption Behavior.* Hershey, PA: IGI Global.

Shenton, A. K., 2004. Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information,* Volume 22, p. 63–75.

Shoib, G., Nandhakumar, J. & Jones, M., 2006. *Using Social Theory In Information Systems Research: A Reflexive Account, in Qualityand Impact of Qualitative Research.* Brisbane, Institute for Integrated and Intelligent Systems, Griffith University, pp. 129-147.

Sikolia, D., Biros, D., Mason, M. & Weiser, M., 2013. *Trustworthiness of Grounded Theory Methodology Research in Information Systems.* s.l., s.n.

Sinclair, A., 1993. Approaches to organisational culture and ethics. *Journal of Business Ethics,* 12(1), p. 63–73.

Siponen, M., Adam, M. M. & Pahnila, S., 2014. Employees' adherence to information security policies: An exploratory field study. *Information and Management,* 51(2), pp. 217-224.

Siponen, M., Pahnila, S. & Mahmood, M. A., 2010. Compliance with information security policies: An empirical investigation. *Computer,* 43(2), pp. 64-71.

Siponen, M. T., 2000. A conceptual foundation for organizational information security awareness. *Information Management & Computer Security,* 8(1), pp. 31-41.

Siponen, M. & Vance, A., 2010. Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly,* 34(3), pp. 487-502.

Sirma, J., Muiru, M. & Kipchillat, C., 2014. Impact of Information Security Policies on Computer Security Breach Incidences in Kenyan Public Universities. *Information and Knowledge Management,* 4(9), pp. 42-49.

Smircich, L., 1983. Concepts of Culture and Organizational Analysis. *Administrative Science Quarterly,* 28(3), pp. 339-358.

Smith, M. L., 2006. Overcoming theory-practice inconsistencies: Critical realism and information systems research. *Information and Organization,* 16(2006), p. 191–211.

Sommestad, T. & Hallberg, J., 2015. The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information and Computer Security,* 23(2), pp. 200-217.

Sommestad, T., Karlzén, H. & Hallberg, J., 2015. A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour. *International Journal of Information Security and Privacy,* 19(1), pp. 26-46.

Sommestad, T., Karlzén, H. & Hallberg, J., 2019. The Theory of Planned Behavior and Information Security Policy Compliance. *Journal of Computer Information Systems,* 59(4), pp. 344-353.

Stincelli, E. & Baghurst, T., 2014. A Grounded Theory Exploration of Informal Leadership Qualities as Perceived by Employees and Managers in Small Organizations. *International Journal of Business Management and Economic Research (IJBMER),* 5(1), pp. 1-8.

Strauss, A. L. & Corbin, J. M., 1990. *Basics of Qualitative Research: Grounded Theory Procedures and Techniques.* Newbury Park, CA: Sage Publications.

Sutton, R. I. & Staw, B. M., 1995. What Theory is Not. *Administrative Science Quarterly,* 40(3), pp. 371-384.

Taber, K. S., 2000. Case studies and generalizability: grounded theory and research in science education. *International Journal of Science Education,* 22(5), pp. 469-487.

Tang, M., Li, M. & Zhang, T., 2015. The impacts of organizational culture on information security culture: a case study. *Information Technology and Management,* 17(2).

Technology Engineering Group, 2014. *Insider Threat - Securing the Human Layer of the OSI Stack.* s.l.:s.n.

The Commission for University Education, 2017. *Status of Universities.* [Online] Available at: http://www.cue.or.ke/images/phocadownload/Accredited_Universities_in_Kenya_November_2017.pdf

Thomson, S. B., 2011. Sample Size and Grounded Theory. *Journal of Administration and Governance,* 5(1), pp. 45-52.

Truex, D., Holmström, J. & Keil, M., 2006. Theorizing in information systems research: A reflexive analysis of the adaptation of theory in information systems research. *Journal of the Association for Information Systems,* 7(12), pp. 797-821.

Uddin, M. J., Luva, R. H. & Hossian, S. M., 2013. Impact of Organizational Culture on Employee Performance and Productivity: A Case Study of Telecommunication Sector in Bangladesh. *International Journal of Business and Management,* 8(2), pp. 63 - 77.

Urquhart, C. & Fernánde, W., 2013. Using grounded theory method in information systems: the researcher as blank slate and other myths. *Journal of Information Technology,* 2013(28), p. 224–236.

Urquhart, C., Lehmann, L. & Myers, M. D., 2010. Putting the 'theory' back into grounded theory: guidelines for grounded theory studies in information systems. *Info Systems J,* Volume 20, p. 357–381.

Vaidyanathan, G. & Berhanu, N., 2012. Impact of Security Countermeasures in Organizational Information Convergence: A Theoretical Model. *Issues in Information Systems,* 13(2), pp. 21-25.

Vance, A., Siponen, M. & Pahnila, S., 2012. Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management,* 49(2012), p. 190–198.

Veiga, A. D., 2015. The Influence of Information Security Policies on Information Security Culture: Illustrated through a Case Study. *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015),* p. 22.

Veiga, A. D. & Eloff, J. H., 2007. An Information Security Governance Framework. *Information Systems Management,* Volume 24, p. 361–372.

Verizon Enterprise Solutions, 2015. *The 2015 Data Breach Investigations Report,* s.l.: VERIZON ENTERPRISE SOLUTIONS.

Villiers, M. R., 2005. *Three approaches as pillars for interpretive Information Systems research: development research, action research and grounded theory.* s.l., s.n., pp. 111-120.

Virtue, T. & Rainey, J., 2015. Information Risk Assessment. In: *HCISPP Study Guide.* s.l.:s.n.

Vroom, C. & Solms, R., 2004. Towards information security behavioural compliance. *Computers & Security,* Volume 23, pp. 191-198.

Wade, M. & Hulland, J., 2004. The resource-based view and information systems research: Review, extension, and suggestions for future research. *MIS quarterly,* 28(1), pp. 107-142.

Walsham, G., 2006. Doing interpretive research. *European Journal of Information Systems,* Volume 15, p. 320–330.

Wechuli, A. N., Muketha, G. M. & Matoke, N., 2014. Survey of Cyber Security Frameworks. *International Journal of Technology in Computer Science & Engineering,* June, 1(2), pp. 33 - 39.

Werlinger, R., Hawkey, K. & Beznosov, K., 2009. An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security,* 17(1), pp. 4-19.

Whetten, D. A., 1989. What Constitutes a Theoretical Contribution?. *The Academy of Management Review,* October, 14(4), pp. 490-495.

Whitty, M., Doodson, J., Creese, S. & Hodges, D., 2015. Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords. *Cyberpsychol Behav Soc Netw,* 18(1), p. 3–7.

Williams, B., Brown, T. & Onsman, A., 2012. Exploratory factor analysis: A five-step guide for novices. *Australasian Journal of Paramedicine,* 8(3), pp. 1-13.

Willison, R. & Warkentin, M., 2013. Beyond Deterrence: An Expanded View of Employee Computer Abuse. *MIS Quarterly,* March, 37(1), pp. 1-20.

Workman, M., Bommer, W. H. & Straub, D., 2008. Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior,* p. 2799–2816.

APPENDIX 1: Interview Questions for the Selected Cases

Open-ended interview questions guide for management

1. Can you briefly describe your organization's Information Security Policy in a summary in terms of its objectives and means to achieve the objectives?

2. Briefly describe the Structure of Information Security arrangements in your organization (*You are free to omit any sensitive information in this question*)

3. Can you highlight how your organization handles insiders who infringe or go against the laid down information security policies if at all you have ever had such a case?

4. How does your organization deal with incidents of staff committing insider instigated infringements?

5. How would you describe the information security cultures or shared values in your organization?

6. Can you describe what kind of strategies your organization has with regards to the overview and revision of the existing policies?

7. As a manager, how would you describe the Management support for information security policy in this organization?

8. At times environment that an organization operates in has an impact on how the organization fulfils policy compliance, can you briefly explain how the environment your organization is in has affected how you make decisions on information security compliance?

9. How about the technological climate that universities and institutions like yours operate in, what would you say are the determining factors that drive what kind of decisions the management make with regards to information security compliance?

Thank you for your time. It has been a very informative session and still looking forward to future engagements.

Open-ended interview questions guide for Information Technology staff and Professionals in the organization

1. Can you briefly describe your organization's information security policy in terms of addressing information security challenges?

2. How does your organization deal with any compliance issues?

3. Briefly describe the Structure of information security arrangements in your organization

4. How can you explain the response by your organization Insiders infringe or go against the laid down Information Security policies?

5. How would you describe the information security cultures or shared values in your organization?

6. If you were to have an opinion on compliance with information security in your organization, how would you describe the organizational adherence to the information security policies?

7. How often does your organization do an overview and revision of the existing policies?

8. How would you describe the organization's staff response to these changes when they occur?

9. As a professional or an IT staff, how would you explain the level of awareness and understanding of the laid down information security policy regulations by your colleagues?

10. As a staff, how would you describe the culture towards information security compliance?

Thank you for your time. It has been a very informative session and still looking forward to future engagements.

Open-ended interview questions guide for normal staff and students in the organization

1. Can you briefly describe your organization's information security policy if in terms of addressing information security challenges if you are aware of any?

2. Briefly describe the structure of information security arrangements in your organization

3. How does your organization deal with any compliance issues?

4. How would you describe the information security cultures or shared values in your organization?

5. How often does your organization do an overview and revision of the existing policies and what informs the review action?

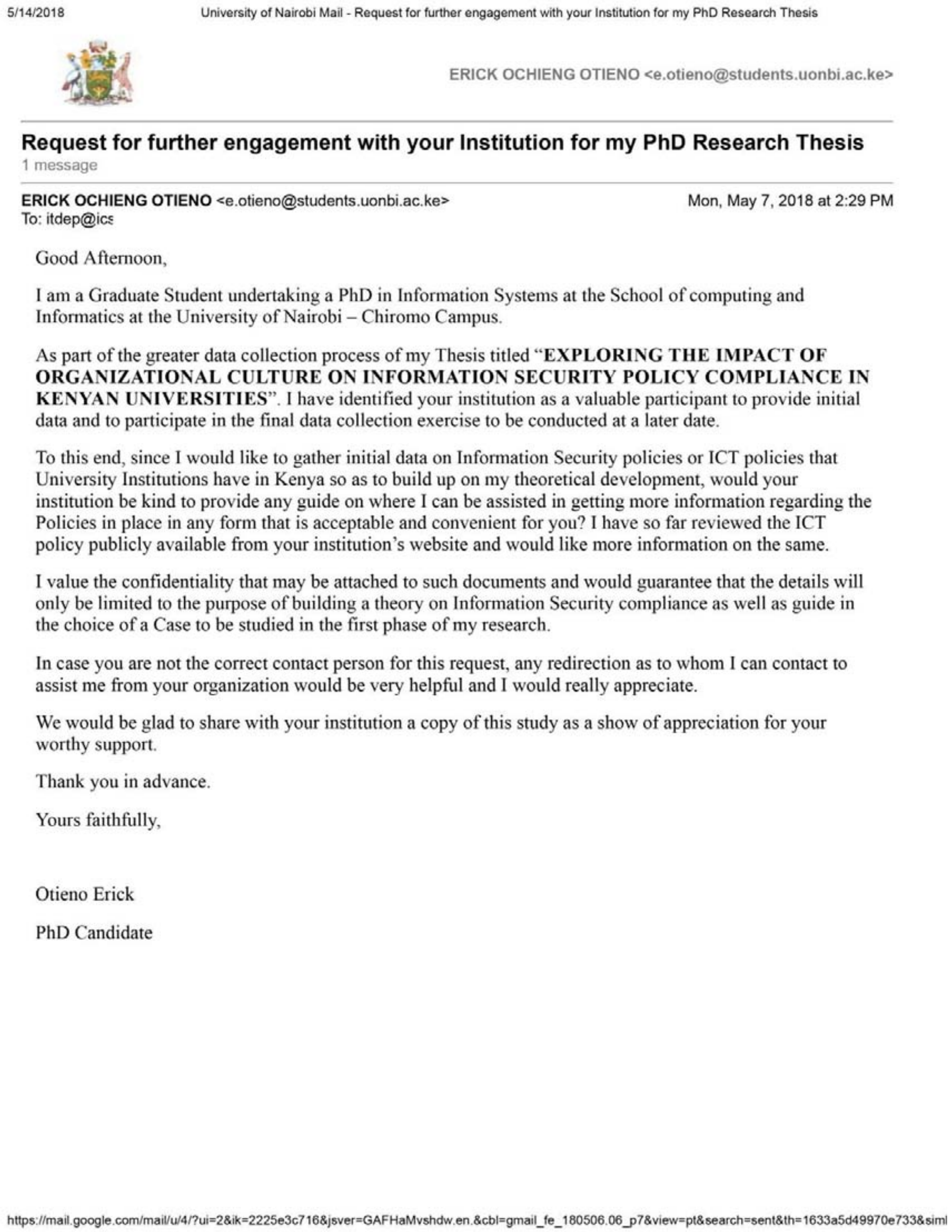
6. As a staff in this organization, how would you describe the management support for Information Security policy in this organization?

7. How about the other staff including those in your field, how would you describe the level of awareness and understanding of the laid down information security policy regulations by your colleagues?

8. As a staff, how would you explain the culture towards information security compliance?

Thank you for your time. It has been a very informative session and still looking forward to future engagements.

APPENDIX 2: Introductory Letters to the Universities Requesting for Information



5/14/2018 University of Nairobi Mail - Request for further engagement with your Institution for my PhD Research Thesis

ERICK OCHIENG OTIENO <e.otieno@students.uonbi.ac.ke>

Request for further engagement with your Institution for my PhD Research Thesis

1 message

ERICK OCHIENG OTIENO <e.otieno@students.uonbi.ac.ke> Mon, May 7, 2018 at 2:29 PM

To: itdep@ics

Good Afternoon,

I am a Graduate Student undertaking a PhD in Information Systems at the School of computing and Informatics at the University of Nairobi – Chiromo Campus.

As part of the greater data collection process of my Thesis titled "**EXPLORING THE IMPACT OF ORGANIZATIONAL CULTURE ON INFORMATION SECURITY POLICY COMPLIANCE IN KENYAN UNIVERSITIES**". I have identified your institution as a valuable participant to provide initial data and to participate in the final data collection exercise to be conducted at a later date.

To this end, since I would like to gather initial data on Information Security policies or ICT policies that University Institutions have in Kenya so as to build up on my theoretical development, would your institution be kind to provide any guide on where I can be assisted in getting more information regarding the Policies in place in any form that is acceptable and convenient for you? I have so far reviewed the ICT policy publicly available from your institution's website and would like more information on the same.

I value the confidentiality that may be attached to such documents and would guarantee that the details will only be limited to the purpose of building a theory on Information Security compliance as well as guide in the choice of a Case to be studied in the first phase of my research.

In case you are not the correct contact person for this request, any redirection as to whom I can contact to assist me from your organization would be very helpful and I would really appreciate.

We would be glad to share with your institution a copy of this study as a show of appreciation for your worthy support.

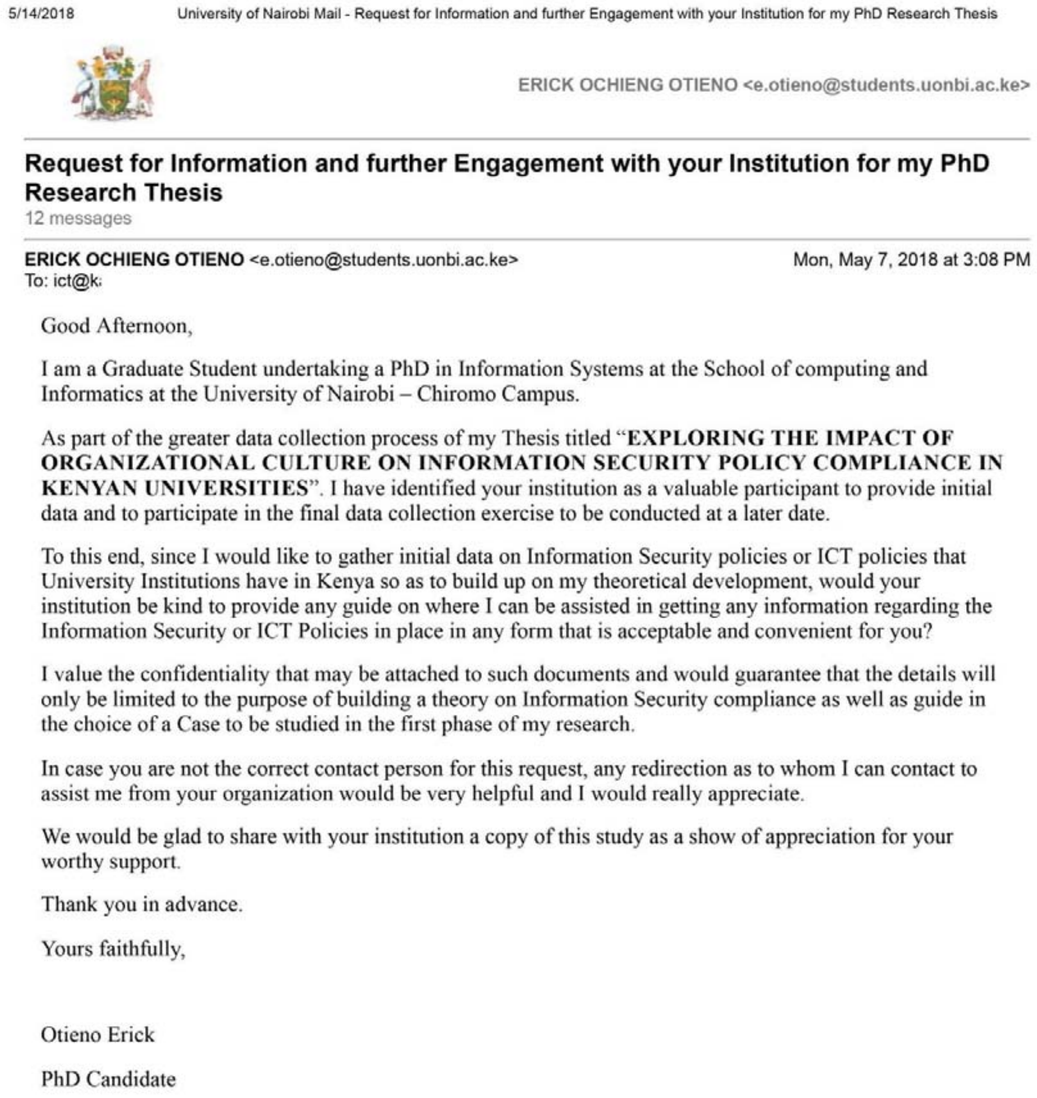
Thank you in advance.

Yours faithfully,

Otieno Erick

PhD Candidate

https://mail.google.com/mail/u/4/?ui=2&ik=2225e3c716&jsver=GAFHaMvshdw.en.&cbl=gmail_fe_180506.06_p7&view=pt&search=sent&th=1633a5d49970e733&siml



5/14/2018 University of Nairobi Mail - Request for Information and further Engagement with your Institution for my PhD Research Thesis

ERICK OCHIENG OTIENO <e.otieno@students.uonbi.ac.ke>

Request for Information and further Engagement with your Institution for my PhD Research Thesis

12 messages

ERICK OCHIENG OTIENO <e.otieno@students.uonbi.ac.ke> Mon, May 7, 2018 at 3:08 PM
To: ict@k

Good Afternoon,

I am a Graduate Student undertaking a PhD in Information Systems at the School of computing and Informatics at the University of Nairobi – Chiromo Campus.

As part of the greater data collection process of my Thesis titled "**EXPLORING THE IMPACT OF ORGANIZATIONAL CULTURE ON INFORMATION SECURITY POLICY COMPLIANCE IN KENYAN UNIVERSITIES**". I have identified your institution as a valuable participant to provide initial data and to participate in the final data collection exercise to be conducted at a later date.

To this end, since I would like to gather initial data on Information Security policies or ICT policies that University Institutions have in Kenya so as to build up on my theoretical development, would your institution be kind to provide any guide on where I can be assisted in getting any information regarding the Information Security or ICT Policies in place in any form that is acceptable and convenient for you?

I value the confidentiality that may be attached to such documents and would guarantee that the details will only be limited to the purpose of building a theory on Information Security compliance as well as guide in the choice of a Case to be studied in the first phase of my research.

In case you are not the correct contact person for this request, any redirection as to whom I can contact to assist me from your organization would be very helpful and I would really appreciate.

We would be glad to share with your institution a copy of this study as a show of appreciation for your worthy support.

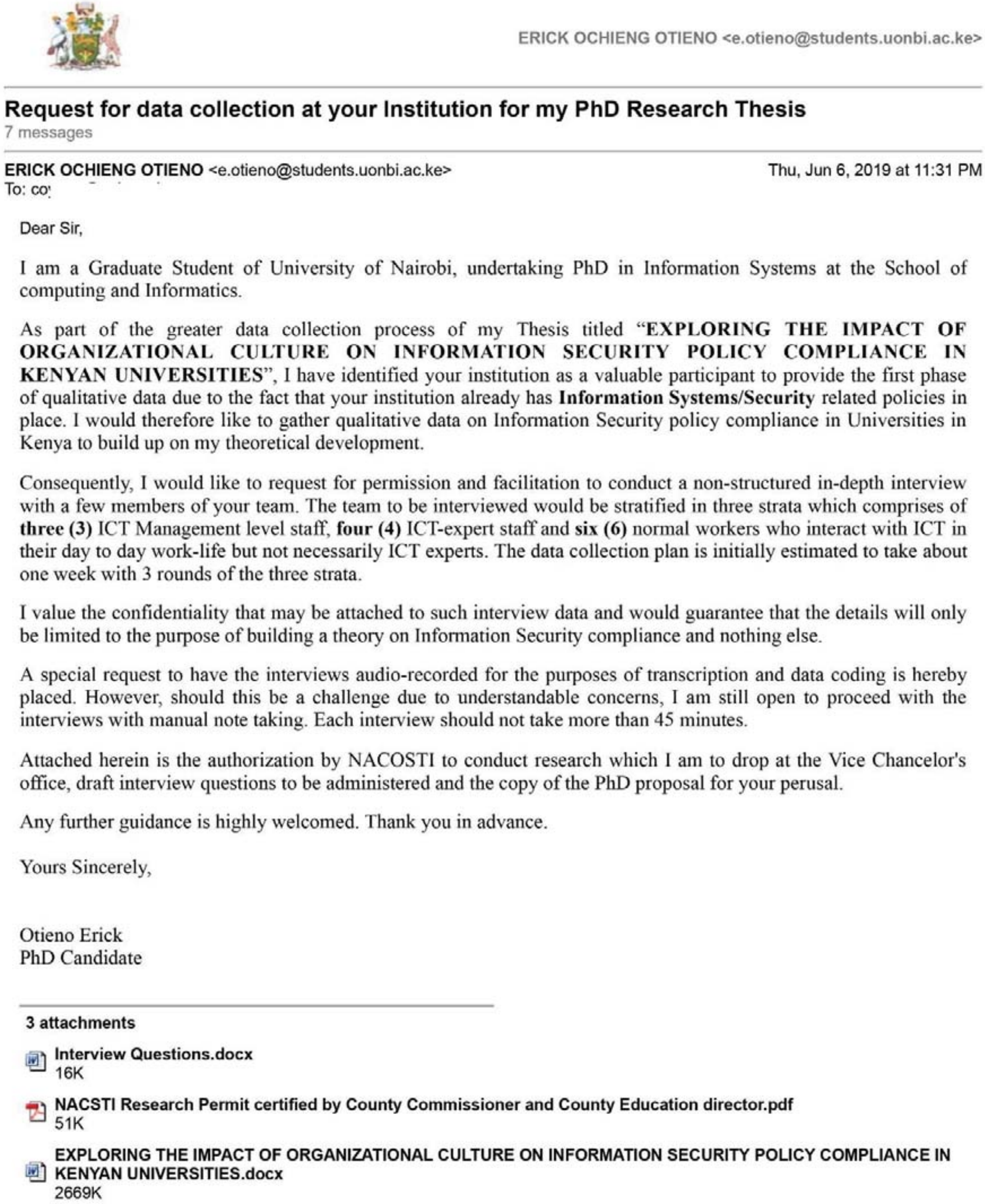
Thank you in advance.

Yours faithfully,

Otieno Erick

PhD Candidate

APPENDIX 3: Request Letter to Universities to Collect Data



ERICK OCHIENG OTIENO <e.otieno@students.uonbi.ac.ke>

Request for data collection at your Institution for my PhD Research Thesis
7 messages

ERICK OCHIENG OTIENO <e.otieno@students.uonbi.ac.ke> Thu, Jun 6, 2019 at 11:31 PM
To: co

Dear Sir,

I am a Graduate Student of University of Nairobi, undertaking PhD in Information Systems at the School of computing and Informatics.

As part of the greater data collection process of my Thesis titled "**EXPLORING THE IMPACT OF ORGANIZATIONAL CULTURE ON INFORMATION SECURITY POLICY COMPLIANCE IN KENYAN UNIVERSITIES**", I have identified your institution as a valuable participant to provide the first phase of qualitative data due to the fact that your institution already has **Information Systems/Security** related policies in place. I would therefore like to gather qualitative data on Information Security policy compliance in Universities in Kenya to build up on my theoretical development.

Consequently, I would like to request for permission and facilitation to conduct a non-structured in-depth interview with a few members of your team. The team to be interviewed would be stratified in three strata which comprises of **three (3)** ICT Management level staff, **four (4)** ICT-expert staff and **six (6)** normal workers who interact with ICT in their day to day work-life but not necessarily ICT experts. The data collection plan is initially estimated to take about one week with 3 rounds of the three strata.

I value the confidentiality that may be attached to such interview data and would guarantee that the details will only be limited to the purpose of building a theory on Information Security compliance and nothing else.

A special request to have the interviews audio-recorded for the purposes of transcription and data coding is hereby placed. However, should this be a challenge due to understandable concerns, I am still open to proceed with the interviews with manual note taking. Each interview should not take more than 45 minutes.

Attached herein is the authorization by NACOSTI to conduct research which I am to drop at the Vice Chancelor's office, draft interview questions to be administered and the copy of the PhD proposal for your perusal.

Any further guidance is highly welcomed. Thank you in advance.

Yours Sincerely,

Otieno Erick
PhD Candidate

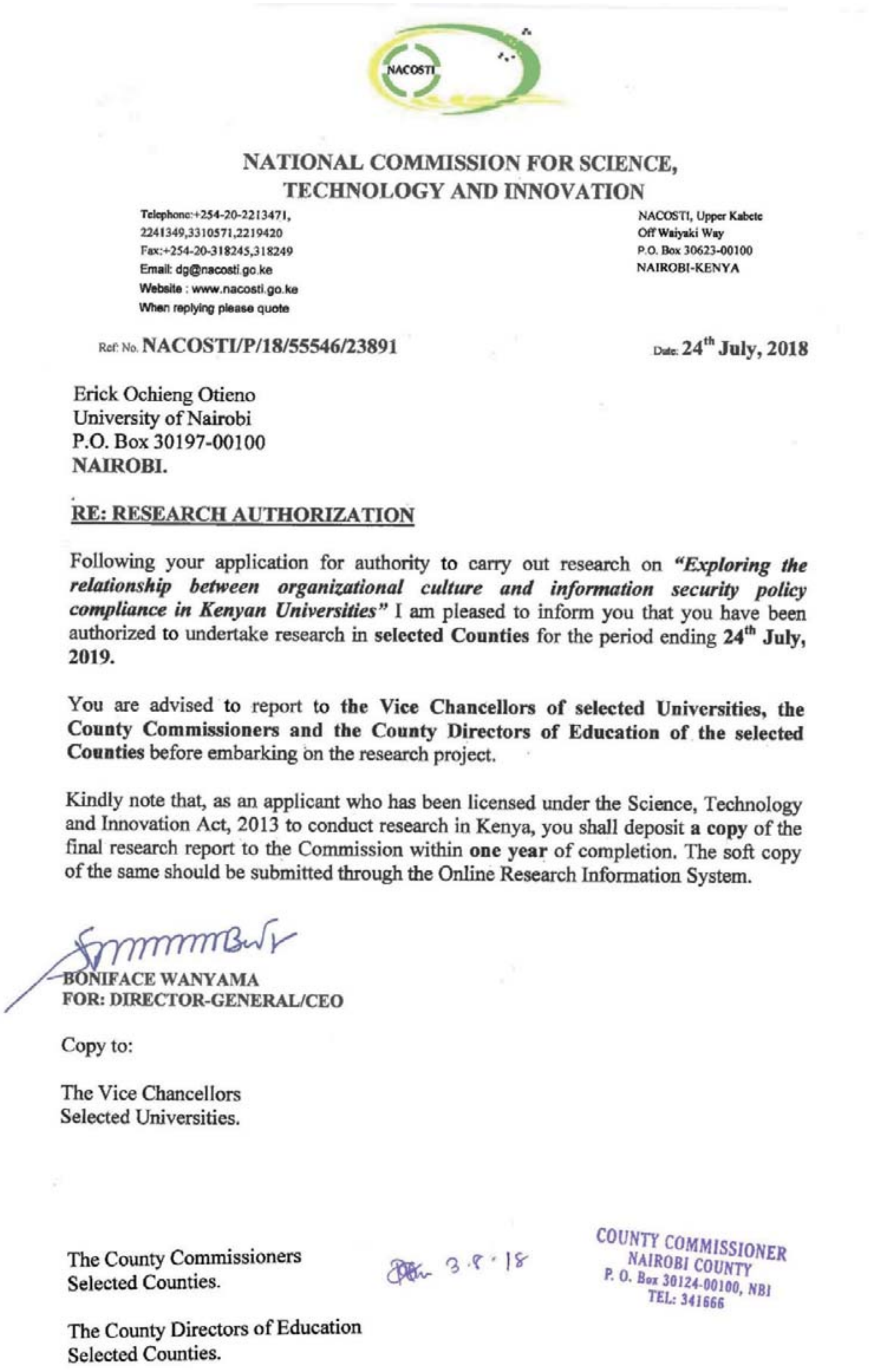
3 attachments

Interview Questions.docx
16K

NACSTI Research Permit certified by County Commissioner and County Education director.pdf
51K

EXPLORING THE IMPACT OF ORGANIZATIONAL CULTURE ON INFORMATION SECURITY POLICY COMPLIANCE IN KENYAN UNIVERSITIES.docx
2669K

APPENDIX 4: NACOSTI Letter of Authorization to Research in Phase One



NACOSTI

NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY AND INNOVATION

Telephone:+254-20-2213471,
2241349,3310571,2219420
Fax:+254-20-318245,318249
Email: dg@nacosti.go.ke
Website : www.nacosti.go.ke
When replying please quote

NACOSTI, Upper Kabete
Off Waiyaki Way
P.O. Box 30623-00100
NAIROBI-KENYA

Ref: No. **NACOSTI/P/18/55546/23891**

Date: **24th July, 2018**

Erick Ochieng Otieno
University of Nairobi
P.O. Box 30197-00100
NAIROBI.

RE: RESEARCH AUTHORIZATION

Following your application for authority to carry out research on ***"Exploring the relationship between organizational culture and information security policy compliance in Kenyan Universities"*** I am pleased to inform you that you have been authorized to undertake research in **selected Counties** for the period ending **24th July, 2019.**

You are advised to report to **the Vice Chancellors of selected Universities, the County Commissioners and the County Directors of Education of the selected Counties** before embarking on the research project.

Kindly note that, as an applicant who has been licensed under the Science, Technology and Innovation Act, 2013 to conduct research in Kenya, you shall deposit **a copy** of the final research report to the Commission within **one year** of completion. The soft copy of the same should be submitted through the Online Research Information System.

BONIFACE WANYAMA
FOR: DIRECTOR-GENERAL/CEO

Copy to:

The Vice Chancellors
Selected Universities.

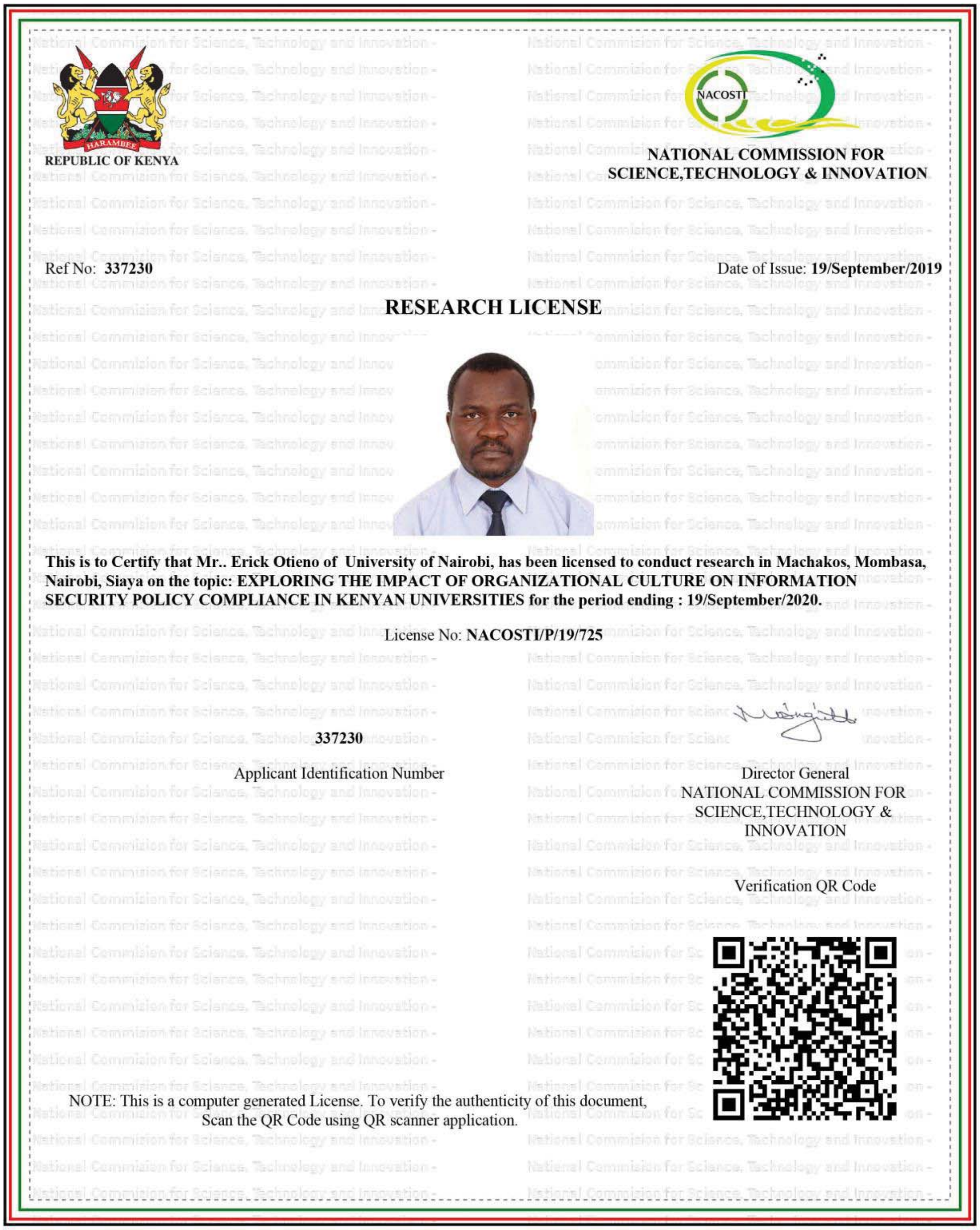
The County Commissioners
Selected Counties.

3.8.18

COUNTY COMMISSIONER
NAIROBI COUNTY
P. O. Box 30124-00100, NBI
TEL: 341666

The County Directors of Education
Selected Counties.

APPENDIX 5: NACOSTI Letter of Authorization to Research in Phase Two



REPUBLIC OF KENYA

NATIONAL COMMISSION FOR
SCIENCE,TECHNOLOGY & INNOVATION

Ref No: **337230**

Date of Issue: **19/September/2019**

RESEARCH LICENSE

This is to Certify that Mr.. Erick Otieno of University of Nairobi, has been licensed to conduct research in Machakos, Mombasa, Nairobi, Siaya on the topic: EXPLORING THE IMPACT OF ORGANIZATIONAL CULTURE ON INFORMATION SECURITY POLICY COMPLIANCE IN KENYAN UNIVERSITIES for the period ending : 19/September/2020.

License No: **NACOSTI/P/19/725**

337230

Applicant Identification Number

Director General
NATIONAL COMMISSION FOR
SCIENCE,TECHNOLOGY &
INNOVATION

Verification QR Code

NOTE: This is a computer generated License. To verify the authenticity of this document,
Scan the QR Code using QR scanner application.

APPENDIX 6: Identified Information Security Compliance Antecedents

Table 28: Identified information security compliance antecedents

Identified Antecedents/Predictors	**Citation**	**Antecedents /Predictors internal to the organizational information security compliance**		
		Organizational level applicability	**Social/behavioral level applicability**	**Technological level applicability**
Anticipated Regret among individuals	(Sommestad, et al., 2015)		+	
Appraisal Cognitive Processes	(Vance, et al., 2012)		+	
Attitude	(Safa, et al., 2016)		+	
Attitude by individuals	(Bulgurcu, et al., 2010)		+	
Attitudes of the employees	(Pahnila, et al., 2007)		+	
Attitudes towards compliance	(Ifinedo, 2014)		+	
Awareness Program	(D'Arcy, et al., 2009)		+	
Breach severity perception	(Herath & Rao, 2009)		+	
Coercive external pressure	(Hu, et al., 2007)	+		
Coercive Pressures	(AlKalbani, et al., 2017)	+	+	
Cognitive Processes of an individual	(Hu, Dinev, Hart, & Cooke, 2012)		+	
Coping Appraisals	(Vance, et al., 2012)		+	
Coping Efficacy	(Hwang & Lee, 2016)		+	
Employees' Capabilities	(Ifinedo, 2014)		+	
Employees' Competence	(Ifinedo, 2014)		+	
Formal Sanctions	(Siponen & Vance, 2010)		+	
Goal Setting	(Hwang & Lee, 2016)	+	+	
Habit	(Vance, et al., 2012)		+	

Identified Antecedents/Predictors	**Citation**	**Antecedents /Predictors internal to the organizational information security compliance**		
		Organizational level applicability	**Social/behavioral level applicability**	**Technological level applicability**
Habits of the employees	(Pahnila, Siponen, & Mahmood, 2007)		+	
Individual beliefs	(Bulgurcu, et al., 2010)		+	
Individual Shame	(Siponen & Vance, 2010)		+	
Individual social interactions	(Herath & Rao, 2009)		+	
Individual's Moral Beliefs	(Hu, Xu, Dinev, & Ling, 2011)		+	
Informal Sanctions	(Siponen & Vance, 2010)		+	
Information Security Awareness	(Karydaa, Kiountouzisa, & Kokolakis, 2005)		+	
Information Security Awareness	(Puhakainen & Siponen, 2010)		+	
Information Security awareness programs	(Bulgurcu, et al., 2010)		+	
Internal social setup	(Hu, et al., 2007)	+	+	
Involvement, Attachment, Commitment, Personnel Norms	(Safa, et al., 2016)		+	
Locus of Control	(Ifinedo, 2014)	+		
Mimetic pressures	(Hu, et al., 2007)	+		
Mimetic Pressures	(AlKalbani, et al., 2017)	+		
Neutralization	(Siponen & Vance, 2010)	+		
Normative beliefs	(Bulgurcu, Cavusoglu, & Benbasat, 2010)		+	
Normative beliefs of the employees	(Pahnila, Siponen, & Mahmood, 2007)		+	

Identified Antecedents/Predictors	Citation	Antecedents /Predictors internal to the organizational information security compliance		
		Organizational level applicability	Social/behavioral level applicability	Technological level applicability
Normative external pressure	(Hu, et al., 2007)	+		
Normative Pressures	(AlKalbani, et al., 2017)		+	
Openness to change	(Myyry, Siponen, Pahnila, Vartiainen, & Vance, 2009)	+	+	
Organizational commitment	(Herath & Rao, 2009)	+		
Organizational Culture	(Karydaa, Kiountouzisa, & Kokolakis, 2005)	+		
Organizational Culture	(Hu, Dinev, Hart, & Cooke, 2012)	+		
Organizational environment	(Chan, Woon, & Kankanhalli, 2005)	+		
Organizational resource availability	(Herath & Rao, 2009)	+		
Organizational structure	(Karydaa, Kiountouzisa, & Kokolakis, 2005)	+		
Penalties Severity	(Herath & Rao, 2009)		+	
Perceived Benefits	(Hu, Xu, Dinev, & Ling, 2011)		+	
perceived ease of technology	(Workman, Bommer, & Straub, 2008)			+
Perceived effectiveness	(Workman, Bommer, & Straub, 2008)		+	
Perceived effectiveness of one’s action	(Herath & Rao, 2009)		+	
Perceived Risks	(Hu, Xu, Dinev, & Ling, 2011)		+	
Perceived threat severity	(Johnston & Warkentin, 2010)		+	
Perceived threat susceptibility	(Johnston & Warkentin, 2010)		+	

Identified Antecedents/Predictors	**Citation**	**Antecedents /Predictors internal to the organizational information security compliance**		
		Organizational level applicability	**Social/behavioral level applicability**	**Technological level applicability**
Perceived threats levels	(Workman, Bommer, & Straub, 2008)		+	
Perception of Information Security Climate	(Chan, Woon, & Kankanhalli, 2005)	+	+	
Possibility of Detection	(Herath & Rao, 2009)		+	
Preconvention reasoning	(Myyry, Siponen, Pahnila, Vartiainen, & Vance, 2009)		+	
Self-Control	(Hu, Xu, Dinev, & Ling, 2011)		+	
Self-Efficacy	(Chan, Woon, & Kankanhalli, 2005)		+	
Social bonds	(Ifinedo, 2014)	+	+	
Social influence of an individual	(Johnston & Warkentin, 2010)		+	
Social pressures upon individuals	(Herath & Rao, 2009)		+	
Subjective norms	(Ifinedo, 2014)		+	
Threat appraisal	(D'Arcy, Hovav, & Galletta, 2009)		+	
Threat appraisal by the employees in an organization	(Pahnila, Siponen, & Mahmood, 2007)		+	
Threat Appraisal Process	(Sommestad, et al., 2015)		+	
Top Management	(Hu, Dinev, Hart, & Cooke, 2012)	+		
Top management Support and buy-in	(Karydaa, Kiountouzisa, & Kokolakis, 2005)	+		

APPENDIX 7: Survey Questionnaire, Hypothesis and Key Indicators, Construct Operationalization

Operationalization of hypothesized constructs from the emergent themes

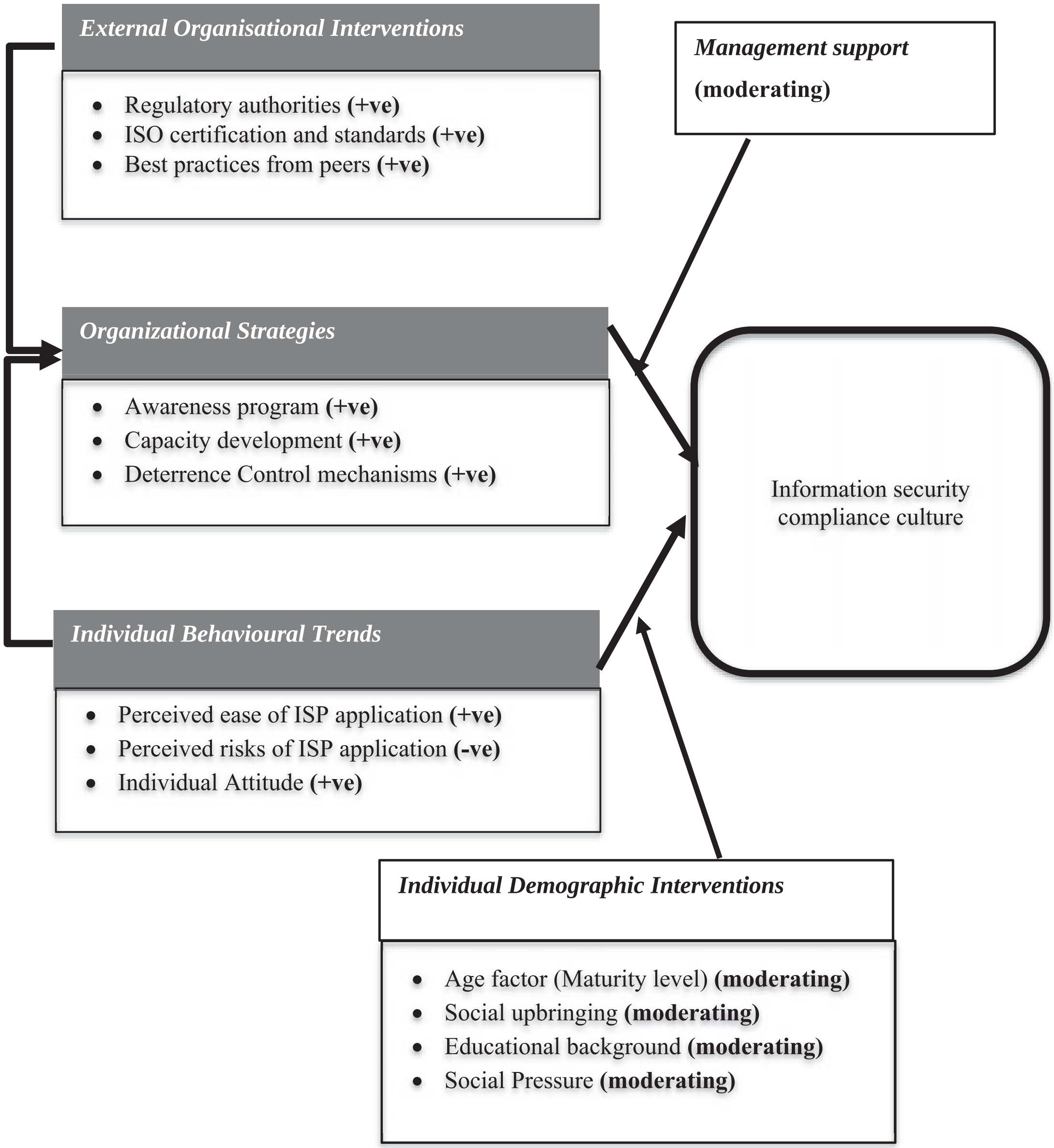

External Organisational Interventions
Regulatory authorities (+ve)
ISO certification and standards (+ve)
Best practices from peers (+ve)
Management support (moderating)
Organizational Strategies
Awareness program (+ve)
Capacity development (+ve)
Deterrence Control mechanisms (+ve)
Information security compliance culture
Individual Behavioural Trends
Perceived ease of ISP application (+ve)
Perceived risks of ISP application (-ve)
Individual Attitude (+ve)
Individual Demographic Interventions
Age factor (Maturity level) (moderating)
Social upbringing (moderating)
Educational background (moderating)
Social Pressure (moderating)

Figure 42: Compiled Operationalization of the Multi-Level model for interactions between organizational strategies, individual behavioral trend, and Information security compliance culture (Source: Research)

Construct operationalization

Constructs	Operationalization Type	Hypothesis
Information security compliance culture	Reflective	
Demographic Moderating factors		
Age factor (Maturity Level) **(AF)**	Moderating	**H1:** Age has a moderating effect between *Individual Demographic Interventions* and *information security compliance culture*.
Social upbringing **(SU)**	Moderating	**H2:** Social upbringing has a moderating effect between *Individual Demographic Interventions* and *information security compliance culture*.
Social pressure **(SP)**	Moderating	**H3:** Social pressure has a moderating effect between *Individual Demographic Interventions* and *information security compliance culture*.
Educational background **(EB)**	Moderating	**H4:** Education background has a moderating effect between *Individual Demographic Interventions* and *information security compliance culture*.
Organizational Moderating factors		
Management support **(MS)**	Moderating	**H5:** Management support has a moderating effect between *Organisational External Interventions* and *information security compliance culture*.
External Organisational Interventions		
Regulatory authorities **(RA)**	Reflective **(+ve)**	**H6:** Regulatory authorities influence organizational initiatives towards information security compliance
ISO certification and standards **(ISO-CS)**	Reflective **(+ve)**	**H7:** ISO certification and standards influence organizational initiatives towards information security compliance
Best practices from peers **(BPP)**	Reflective **(+ve)**	**H8:** Best practices from peers influence organizational initiatives towards information security compliance
Organizational initiatives		
Awareness program **(AP)**	Reflective **(+ve)**	**H9:** Awareness program initiative by organizations influences the compliance with information security policies

Constructs	Operationalization Type	Hypothesis
Capacity development **(CD)**	Reflective **(+ve)**	**H10:** Capacity development initiatives by organizations influence information security culture
Deterrence Control mechanisms **(DCM)**	Reflective **(+ve)**	**H11:** The deterrent control initiatives by organizations influences information security compliance culture
Individual Behavioural Trends		
Perceived ease of ISP application **(PEIA)**	Reflective **(-ve)**	**H12:** Perceived ease of ISP application influences the information security compliance culture in organizations
Perceived risks of ISP application **(PRIA)**	Reflective **(-ve)**	**H13:** Perceived risks of ISP application influences information security compliance culture in organizations
Individual attitude, **(IA)**	Reflective **(+ve)**	**H14:** Individual attitude towards the authority influences information security compliance culture

Hypothesis and Key Indicators

Hypothesis	Key Indicators and Coding
H1: Age has a moderating effect between *Individual Demographic Interventions* and *information security compliance culture*.	• Mature staff are more likely to reason and comply with information security policies in place **(DMF-AF1)** • Handling a diverse age group provides a challenging environment when enforcing information security policy **(DMF-AF2)**
H2: Social upbringing to some extent influenced how users complied with information security policies	• The difference in social upbringing provides a big challenge when enforcing information security policies **(DMF-SU1)**
H3: Social pressure has a moderating effect between *Individual Demographic Interventions* and *information security compliance culture*.	• Handling members under seer pressure is challenging when enforcing information security compliance **(DMF-SP1)**
H4: Education background influences information security compliance	• We have challenges enforcing information security policy when dealing with members with a technology background **(DMF-EB1)**
H5: Management support has a moderating effect between *Organisational External Interventions* and *information security compliance culture*.	• Management support improves the execution of information security policies **(OMF-MS1)** • I feel motivated to comply with information security when management also complies **(OMF-MS2)** • It is easier to create awareness when management gets involved in the process **(OMF-MS3)**
H6: Regulatory authorities influence organizational initiatives towards information security compliance	• We are obliged to follow the regulatory authorities' requirements **(EOI-RA1)**
H7: ISO certification and standards influence organizational initiatives towards information security compliance	• External certification obligations increase the level of responsibility to enforce compliance with information security policies **(EOI-ISO-CS1)**
H8: Best practices from peers influence organizational initiatives towards information security compliance	• Learning from peers encourages a well-planned information security compliance initiative **(EOI-BP1)**
H9: Awareness program initiative by organizations influences the compliance with information security policies	• A conscious society increases the level of compliance with information security policies **(OI-AP1)**
H10: Capacity development initiatives by organizations influence information security culture	• Constant training and capacity development encourage members to comply with information security policies **(OS-CD1)**
H11: The deterrent control initiatives by organizations	• Our deterrent initiatives discourage noncompliance behavior **(OS-DC1)**

Hypothesis	Key Indicators and Coding
influences information security compliance culture	• Our control mechanism reduces incidents of non-compliance with information security policies **(OS-DC2)** • Our monitoring initiatives enables the detection of information security breaches in time **(OS-DC3)**
H12: Perceived ease of ISP application influences the information security compliance culture in organizations	• I am more likely to comply when the policies are interventions are easy to understand and use **(IBT-PEIA)**
H13: Perceived risks of ISP application influences information security compliance culture in organizations	• I am more likely to avoid complying with information security policies if I perceive them to be a risk to me or my privacy **(IBT-PRIA)**
H14: Individual attitude influences information security compliance culture	• Rebellious members will more likely violate information security policies **(IBT-IA1)** • My attitude towards the policies will impact how I comply **(IBT-IA2)**

QUESTIONNAIRE STARTS HERE

We appreciate you for taking the time to answer a few questions in this questionnaire which will be valuable in providing insights into the topic under consideration: "*Exploring the Impact of Organizational Culture on Information security compliance in Kenyan Universities*". We value your confidentiality and privacy needs and as such, we assure you that the questions are designed to guarantee maximum anonymity and confidentiality.

The questionnaire is easy to answer, and it would take you only approximately 20 minutes of your time.

Section A:

Demographic information

1.Name of the institution……………………………………………………………………….

2.Gender

I. Male []
II. Female []

3. What is the category of your age?

I. < 20 []
II. 20-30 []
III. 31-40 []
IV. 41-50 []
V. 50 []

4. Occupation

5. Highest level of educational attainment

I. Non-formal []
II. Primary []
III. Secondary []
IV. Vocational []
V. Tertiary (Polytechnic, University) []
VI. Others, specify______________

6. For how long have you been in the institution?

I. < 1 year []
II. 1-5 years []
III. 5-10 years []
IV. >10years []

Section B:

Background Information Data (Control Variables)

This section is to help us understand your organizational information security policy grounding and ascertain the depth in which the culture of information security interactions is ingrained and a few other details to know how to categorize the statistical results below.

1. **(CTRL-Var1) – Does your University have Information Security related policy(s) in place?**

(*Please choose only one of the following*)

I. Yes []
II. No []
III. I am not willing to disclose []
I don't know []

2. **(CTRL-Var2) - What is your relationship with the University?**

I. I am a Staff at the managerial level []
II. I am a Staff at in the ICT related department []
III. I am a Staff at a department not related to ICT []
I am a student at the University []

3. **(CTRL-Var3) – How long have you been at the University?**

I. 0 to 5 years []
II. 5 to 10 years []
III. 10 to 15 years []
IV. 15 to 20 years []
V. More than 20 years []

4. **(CTRL-Var4) – Has your institution ever experienced any information security-related breaches in the last 10years?**

I. Yes []
II. No []
III. I am not willing to disclose []
IV. I don't know []

5. **(CTRL-Var5) – Has often does your university create awareness on information security policies?**

I. more than 5 times a year []
II. Less than 5 times a year []
III. I have never seen any attempt []
IV. I don't know []

6. **(CTRL-Var6) – Do you believe there is an Information security compliance culture in our university?**

I. Yes, I believe we have an established culture of information security compliance culture []
II. No, I do not believe we have an established culture of information security compliance culture []
III. I do not know about any established culture of information security compliance culture []

Section B:

These questions require you to indicate what scale represents your agreement or disagreement with the statement. The scale is a '7' point strength to enable you to indicate varied measurements. You only need to tick what expresses your view.

Below is a 7-point Linkert Scale.

1	2	3	4	5	6	7
Strongly disagree	Quite Disagree	Slightly Disagree	Neither Agree nor disagree	Slightly Agree	Quite agree	Strongly agree

Please indicate to what extent you agree or disagree with the statements below based on the scale ranging from ***1- (strongly disagree)*** *to* ***7 – (strongly agree)***

B (i) Demographic factors

7. **To what extent would you agree or disagree with the following views regarding Demographic factors influencing information security compliance culture?**

	Strongly disagree 1	**Quite Disagree 2**	**Slightly Disagree 3**	**Neither Agree nor Disagree 4**	**Slightly Agree 5**	**Quite Agree 6**	**Strongly agree 7**
• Mature staff are more likely to reason and comply with information security policies in place **(DMF-AF1)**							
• Handling a diverse age group provides a challenging environment when enforcing information security policy **(DMF-AF2)**							
• The difference in social upbringing provides a big challenge when enforcing							

	Strongly disagree 1	**Quite Disagree 2**	**Slightly Disagree 3**	**Neither Agree nor Disagree 4**	**Slightly Agree 5**	**Quite Agree 6**	**Strongly agree 7**
information security policies **(DMF-SU1)**							
• Handling members under seer pressure is challenging when enforcing information security compliance **(DMF-SP1)**							
• We have challenges enforcing information security policy when dealing with members with a technology background **(DMF-EB1)**							

B (ii) External Organizational Pressure

8. **To what extent would you agree or disagree with the following views regarding External Pressure factors influencing information security compliance culture?**

	Strongly disagree 1	**Quite Disagree 2**	**Slightly Disagree 3**	**Neither Agree nor Disagree 4**	**Slightly Agree 5**	**Quite Agree 6**	**Strongly agree 7**
• We are obliged to follow the regulatory authorities' requirements **(EOI-RA1)**							
• External certification obligations increase the level of responsibility to enforce compliance with information security policies **(EOI-ISO-CS1)**							
• Learning from peers encourages a well-planned information security compliance initiative **(EOI-BP1)**							

B (iii) Organizational Aspects

9. **To what extent would you agree or disagree with the following views regarding Organizational Initiative factors influencing information security compliance culture?**

	Strongly disagree 1	**Quite Disagree 2**	**Slightly Disagree 3**	**Neither Agree nor Disagree 4**	**Slightly Agree 5**	**Quite Agree 6**	**Strongly agree 7**
• Management support improves the execution of information security policies **(OMF-MS1)**							
• I feel motivated to comply with information security when management also complies **(OMF-MS2)**							
• It is easier to create awareness when management gets involved in the process **(OMF-MS3)**							
• A conscious society increases the level of compliance with information security policies **(OI-AP1)**							
• Constant training and capacity development encourage members to comply with information security policies **(OI-CD1)**							

	Strongly disagree 1	**Quite Disagree 2**	**Slightly Disagree 3**	**Neither Agree nor Disagree 4**	**Slightly Agree 5**	**Quite Agree 6**	**Strongly agree 7**
• Our deterrent initiatives discourage noncompliance behavior **(OI-DC1)**							
• Our control mechanism reduces incidents of non-compliance with information security policies **(OI-DC2)**							
• Our monitoring initiatives enables the detection of information security breaches in time **(OI-DC3)**							

B (iv) Individual Behavioural Trends

10. To what extent would you agree or disagree with the following views regarding individual behavioral trends influencing information security compliance culture?

	Strongly disagree 1	**Quite Disagree 2**	**Slightly Disagree 3**	**Neither Agree nor Disagree 4**	**Slightly Agree 5**	**Quite Agree 6**	**Strongly agree 7**
• I am more likely to comply when the policies are interventions are easy to understand and use **(IBT-PEIA)**							

	Strongly disagree 1	**Quite Disagree 2**	**Slightly Disagree 3**	**Neither Agree nor Disagree 4**	**Slightly Agree 5**	**Quite Agree 6**	**Strongly agree 7**
• I am more likely to avoid complying with information security policies if I perceive them to be a risk to me or my privacy **(IBT-PRIA)**							
• Rebellious members will more likely violate information security policies **(IBT-IA1)**							
• My attitude towards the policies will impact how I comply **(IBT-IA2)**							

Thanks a lot for your valuable time and responses.

----END OF QUESTIONNAIRE ----

APPENDIX 8: Theoretical Coding Stage: Emerging Themes and Informant Mapping With Cited Quotes

Theoretical Code: Individual Behavioural Trends		
Selective Code	Cited quote	Informant Mapping
Systems to make working with information security policies assets easy	"…We have managed to create an environment that makes it easy for our colleagues and students to work seamlessly with ICT infrastructure and software with minimal security risks…."	Informant 1: ICT Staff-University A
Technology acceptance initiatives	"…we have hotlines that anybody who has query can reach the IT team on…."	Informant 1: ICT Staff-University A
With the ease of using ICT assets, and making ISPs accessible and easy to understand, compliance has also been on the positive trend	"…We have managed to create an environment that makes it easy for our colleagues and students to work seamlessly with ICT infrastructure and software with minimal security risks. An easy ICT platform to use creates a safer acceptance. And this means that those who use ICT to perform their day to day tasks do not have a reason to compromise on security…."	Informant 1: ICT Staff-University A
Service provision chatter, like a Service Level Agreement (SLA) within the institution	"…For example, there is a process for server administration, for database, for MIS systems, we also have what we call as our chatter…."	Informant 2: ICT-Staff University B
This ensures that everyone knows how and when to expect a service delivery	"…how we provide service, how long does this service when it is requested how long are you supposed to do it…."	Informant 2: ICT-Staff University B

Theoretical Code: Individual Behavioural Trends		
Selective Code	Cited quote	Informant Mapping
Trust is built over time based on the acting capacity basis in which a background check is done in the process	"…Well, we work with different kinds of people, and like I have told you we work more on trust before you are given a docket to manage, also the process of getting there, there has to be long term trust, you have been there in an acting capacity and you have been checked properly. We have not had serious cases internal or maybe someone going against the policy and probably acting against our security measures, but we have once in a while we had had issues of carelessness, someone does something costly, an example is that we use a database in a different section where one is given access to develop and does an update that wipes and messes the systems due to human error but due to backup, we can always…."	Informant 2: ICT-Staff University B
Ease of improving how awareness tools are implemented	"…so, we can use a similar approach to each a wider audience because now that will be delivered right at the workstation of the user. They can do it on demand and then even measure their skills as related security…"	Informant 3: Management level ICT-Staff -University B

Theoretical Code: Individual Behavioural Trends		
Selective Code	Cited quote	Informant Mapping
Attitude towards leadership.	“…Attitude towards leadership. "The way people feel about who is telling them of rules matters a lot. For example, I would my attitude towards leadership would give me the urge to follow with confidence or follow with resentment. I do believe the former is the best. That is why I think having a positive attitude is essential to have people comply"….”	Informant 6: ICT-Student-University B
Attitude towards policy	"…It is all about the will to follow. I am a believer in good leadership and leading from the front. What we are told is the norm needs to follow from everybody. Since I joined the university, I have not seen a situation that makes me feel we are not valued. There are some cases however that students may feel something is amiss in terms of access. But I believe with the proper engagement by the administration, especially the IT department, I feel we have developed positivity to the policies they share with us…."	Informant 9: Student – University A
Perceived ease of applying ISP	“…If it is as simple as ABC, then many will follow the policies. But if the policies themselves are not self-explanatory, then the rationale is lost, and what would be left would be a case of those who want to follow and apply the policy being forced to circumvent it.…”	Informant 11: ICT Student – University B

Theoretical Code: Individual Behavioural Trends		
Selective Code	Cited quote	Informant Mapping
Perceived risks of applying ISP	"…I am more likely to comply if I believe that the policies will not harm me in any way. It is virtually every human instinct. But to say the least, I have not had such options. Here in the university we are treated well and given all avenues to express our difficulties. I have not felt that my rights are infringed like privacy. But should I feel so, I will avoid complying if I can…"	Informant 11: ICT Student – University B
Rebellious attitude towards policy	"…To some extent, students like us are difficult to deal with. If even among ourselves we find it a challenge to work and follow our own rules, I can imagine what the management must contend with. I mean, we have some naturally rebellious students. Even when we are in our groupings like class groups, you will find a few who do not follow what we have all agreed on. And this is hurting and disappointing. When the same students violate information security, they feel good about it…."	Informant 14: Non-ICT Student – University B

Theoretical Code: Individual Behavioural Trends		
Selective Code	Cited quote	Informant Mapping
Perceived risk of applying ISP	"…It is very difficult to follow a rule if you know it will get back to you. Rules, or policies for that matter, should never be used as a tool to harm someone. That, however, is different when I am told in advance that this is what we are collecting, this is what we are using to track, and this is the reason. Do this and Do not do this, and these are the reasons. I that is made clear, I do not think any reasonable person can be mad about it. Policies are there and I, for instance, know that when I log in to the university Wi-Fi, I am openly being monitored. So, it can also act as a deterrence…."	Informant 12: Non-ICT student - University B

Theoretical Code: Individual Demographic Interventions		
Selective Code	Cited quote	Informant Mapping
The nature of students in the institutions are also a factor in the information security management	"…We have very bright students, also one of our challenges and greatest threat, we have very bright students, and most of the bright students doing well outside are from here so once in a while they will try this and that…."	Informant 2: ICT-Staff University B
Though systems are in place to handle this generation of young bright students	"…but then again as I have told you based on how we give rights in the system you will have to try very hard…."	Informant 2: ICT-Staff University B
Dealing with young students on an internship within is challenging Consideration of the demography aspect in handling policy compliance-related issues	"...we have a challenge with the requests for internships and how they access our resources so even when we do grant such, we are also careful on the level of damage…"	Informant 2: ICT-Staff University B
Planning on the worst-case scenario while working with the young and bright interns	"…so will work on the worst-case scenario when we allocate them duties while at the same time helping them to learn. What is the worst if they are given a role what is they can…?"	Informant 2: ICT-Staff University B
Challenges still exist on how to enforce policy on this front	"…which is something we want to welcome but we have recently reviewed a policy around it on the bring your device because we have provided hot spots everywhere so they are accessing through their phones we have places where they can sit, we have labs and laptop is a common thing around the university so we cannot run away from Bring Your Device and we have allowed them.…"	Informant 2: ICT-Staff University B
Lack of interest to read policies by those in the younger generation.	"…But we also face challenges in that people don't read the policy, especially with the young. Though	Informant 4: Management level ICT-Staff-University A

Theoretical Code: Individual Demographic Interventions		
Selective Code	Cited quote	Informant Mapping
	maturity is subjective, and it is more pronounced in those who can reason well with the policy in place….”	
Creative initiatives to handle younger generations in the institution (Demography?)	“…Most of the attacks that we receive are human-engineered so they use the weakness of a person to attack the system then secondly if everybody just complied with laid out standards, you know, if your android does not jailbreak, let me say for students, you know they get creative sometimes and jailbreak then they do that….”	Informant 4: Management level ICT-Staff-University A
Challenges in handling students and the younger generation in the institution, (Demography?)	“…For students, it is another thing. We have that student’s book and it stipulates very well if you intentionally use the information that you must cause harm to the university then you will face the consequences….”	Informant 4: Management level ICT-Staff-University A
The growing ICT trends with regards to social media has brought in more challenges with regards to information security policy management	“…About social media now, that one is usually a bit hard. We have had several attacks you know fake news especially from insiders in students but I believe the majority of the students here really don't delve so much in internal politics because the interest of the person going to social media is either malign down or cause harm to the university. But those who do it we have maybe like took them to court, we ask the company that is hosting the blog to pull down the blog. If it goes further, that is when we go to court or settle out of court or something like that. But is a	Informant 4: Management level ICT-Staff-University A

Theoretical Code: Individual Demographic Interventions		
Selective Code	Cited quote	Informant Mapping
	challenge. Social Media is a challenge….”	
Evidence of what damage can be caused if we cannot manage the younger generation in the institutions	“…Another challenge, that part for demographics, is quite challenging because you can't block like we had tried to block YouTube or video stream consumes a lot like 70% of our traffic is on streaming of videos that costs, we pay almost 30 million Kenya Shillings and you can imagine a quarter of that is what is used for academic matters and the rest is used for entertainment. You see that hurts the organization. Like our social media portal is also locked and you can't just put anything on it, and we put students and who violates we remove from the group….”	Informant 4: Management level ICT-Staff-University A
Generational handling techniques (Demography?)	“…The generation we have today deals with reason and not threat. You threaten them, you encourage them to do it. You tell them these are the consequences of doing this. You bring it down to their level, especially like the ones of computer science that I am dealing with, I will tell them you are going to develop an application. How would you feel if someone posted it online for free, now it makes them think? They put themselves in that situation and they see it wouldn't be fair to them, so why would I do it? for others? I think that is one way. Now the staff, need to have a way of dealing with	Informant 5: Technician Level ICT-Staff-University B

Theoretical Code: Individual Demographic Interventions		
Selective Code	Cited quote	Informant Mapping
	students. We have a very big problem because there is a communication breakdown. We come from a generation where we were told don't do this and you stop. They come from a generation where they are told if you do this, this is what is going to happen. So, you see there is a gap, big one….”	
A structured way of tackling the generational challenges (Demography?)	“…Yes, if you interact with them you will even notice that to some extent, they teach the older generation a lot. These are people who have spent all their time on computers. The older generation only interacted with computers while working. So, there are things they wouldn't know but these young people because they spend all their time on the computer, they will know. If you interact with them from my experience, I have learned a lot from them. I would sit down, and they would tell me, you guys have blocked download of torrents, but my colleagues are still doing it, this is how they are doing it, and they show you. You get to realize that there is a backdoor. But without interacting with them you will just be wondering how comes, you go find a hard disk is full of movies, is full of books, where are they coming from. And we have blocked torrents. It is that they can identify the backdoor….”	Informant 5: Technician Level ICT-Staff-University B

Theoretical Code: Individual Demographic Interventions		
Selective Code	Cited quote	Informant Mapping
Demographic challenges	"…Actually what I have come to realize is that there are those students who we would call them notorious when it comes to the use of machines, they will change your password they will come, in most cases, if you sit down with those students, you will notice they have very small problems. They want to install software, they have talked to the technician, he has refused because he does not understand what this software is for. So, it is very easy to deal with them if you are going to sit down with them and understanding them and they will solve so many of your problems…."	Informant 5: Technician Level ICT-Staff-University B
Ways that have worked in handling the Demographic challenges	"…Because when you talk to them, you get the picture they paint for you. You get to understand, oh, this is what they need because of this. But most of us are older than them and we know, if it is programming you are going to use visual basic or python and that is it. Then they come and tell you a strange name and you are like; I have never heard of that. So, you dismiss them. While if you sat down and listen to them and found out, and they give you their reasons, you will be able to agree…."	Informant 5: Technician Level ICT-Staff-University B
It is easier to handle mature members than the younger generation in the university	"…Addressing challenges of information security with mature students and staff has been much easier since if one understands the rationale of	Informant 5: Technician Level ICT-Staff-University B

Theoretical Code: Individual Demographic Interventions		
Selective Code	Cited quote	Informant Mapping
	restricting some functions and access, they will most likely to comply. The challenges we get mostly are from the ones driven by group dynamics. For example, you will find that some students like downloading a lot of games and videos, and when you restrict them, they end up looking for other avenues of bypassing the restrictions. Though processes and controls are in place, managing the perceptions is equally important….”	
Education background is a factor	“…I have noticed that there needs to be special attention to students from different areas of study. Why am I saying so? Often, students who are in the computer-related studies are more prone to experiment a lot innocently without knowing the exposure they are putting themselves through falling into trap of social engineers on the internet. Many will try to look for software that is restricted and end up going to websites that have malware and viruses. It is however a good thing that our systems and controls are much robust and can detect and prevent any of these attempts. We have had cases where we have asked the students to communicate when they need something that can be useful in enhancing their studies. Students who are in computer science are usually most likely to violate policies due to their	Informant 8: Technician level ICT staff-University A

Theoretical Code: Individual Demographic Interventions		
Selective Code	Cited quote	Informant Mapping
	needs. This is particularly so if they sneak in software that is not allowed. They also know how to crack software as opposed to students in other disciplines….”	
Generational upbringing causing compliance concerns	“…I am a student who is used to social media sharing, and as such, I find it difficult to resist sharing any information that I find interesting to share….”	Informant 19: Student University B
Social Upbringing	“…I grew with a mobile phone from a younger age, and I have never had to be told to comply. I always click anything that is shared….”	Informant 20: Student University B
Peer to peer checks and balances. Everyone knows someone is watching	“…You get the least privilege as possible to enable you to do your work. That is how usually we do it in our culture. Also, we have a culture of trust, but trust is based on roles. For example, if you oversee the database then we entrust you with everything, but within that, we may have a DBA admin model via a DB system admin so there is that responsibility of passing some extra eye to another person….”	Informant 2: ICT-Staff University B
Social Upbringing	“…I have never known that there is something called I always click anything that is shared. When my colleagues share links even those that are not allowed, I am always tempted to click and share too….”	Informant 10: Student – University A
Social Upbringing	“…I believe that social background has a lot to contribute to how policies are complied with. I came from not a well-off family, and I	Informant 12: Non-ICT student - University B

Theoretical Code: Individual Demographic Interventions		
Selective Code	Cited quote	Informant Mapping
	have tried to be as conservative as I possibly can, though, in contrast, I see many of my student colleagues who came from a wealthy background and who had everything in their way. I see them every day….”	
Social Pressure	“…Not. I think the best approach would be for the security managers to understand us, especially this young generation that is very inquisitive, has known only the internet as the source of information, has grown in a very tempting environment of the Internet of Things, and without much guide of what is dangerous out there and what is not….”	Informant 10: Student – University A
Social Pressure	“…I believe I have a basic understanding of cybersecurity issues. But so far, I have not seen any student going as far as hacking. But who knows what happens in the dark? What I have seen is more of the group dynamics. It is evident when you interact with some of my student colleagues. When one can access the allowed sites, everyone will want to do so and even more than just accessing the sites….”	Informant 15: Non-ICT Student – University A
Social Pressure	“…Most of my colleagues will agree with me that what drives us is the group mentality. I know this might sound funny. But I am also time driven by that. I find it mind-boggling to belong even if it may have a negative effect. We go	Informant 19: Student University B

Theoretical Code: Individual Demographic Interventions		
Selective Code	Cited quote	Informant Mapping
	drinking, we go clubbing, and then when we are back in our hostel, we go online on the internet to watch movies. This we do in total disregard for the restrictions that we have. There have been issues raised with internet blockages. But we always find a way around. What do they expect we do? Honestly? I have friends who understand these things. I mean those who are doing computer science. They help us a lot those who are not conversant with these things. We also get videos from them. Do you know the thing about torrents? I know many will say the internet is blocked. But they know how to override the blockade. I think they use a firewall blocker or something like that. Anyway, I do not have much to say about it….”	

Theoretical Code: Organizational Strategies		
Selective Code	Cited quote	Informant Mapping
Initiative to increase awareness	"…We depend a lot on ICT in many situations and as such, we value the security of data that comes with it. So, we have a fully-fledged department that leads to anything ICT including the drafting and enhancing of policies and related action point…."	Informant 1: ICT Staff-University A
Awareness initiatives	"…Well, as I have already indicated, there are those regulations that are shared with all who join the USIU family and we have such regulations in our electronic website for all to access…" "…We have done several awareness initiatives. By this, I mean that any new member of the community is given a briefing on the ICT policies in place…."	Informant 1: ICT Staff-University A

Theoretical Code: Organizational Strategies		
Selective Code	Cited quote	Informant Mapping
Ways to educate and create awareness initiatives	"…The breach that we have had is not perpetrated by insiders per se because you will find maybe someone has opened an email address then he or she clicks and there you have the breach of the system, you see the information is compromised and the computer the user is using starts spamming. you see such a person is innocent and so you can not punish that person. ***But we always try to tell them, do not click***…" "…Well, once we realized there is a malicious email coming in, I am using email because this is what is mostly used, we always send out to say watch out for this, do not click anything like this, this email from this source or this is the way it looks like…."	Informant 4: Management level ICT-Staff-University A
Prospects of awareness working to enhance compliance	"…With my many experiences in IT here in the university and elsewhere, creating awareness to your users is key many violations do not occur because of lack of policies or because people are just stubborn, but at times because they are not aware that they are violating policy. This is more so if you are handling a large group of people with deferent backgrounds…."	Informant 7: ICT-Staff - University A

Theoretical Code: Organizational Strategies		
Selective Code	Cited quote	Informant Mapping
Organization initiative to manage information systems related issues	"…We depend a lot on ICT in many situations and as such, we value the security of data that comes with it. So, we have a fully-fledged department that leads to anything ICT including the drafting and enhancing of policies and related action points. I have never heard of such a breach situation so I would not give any conclusive response…"	Informant 1: ICT Staff-University A
Punishments of breach actions	As an ICT practitioner, I know of different measures that can be taken to such infringements such as preventive measures like different types of punishment.	Informant 1: ICT Staff-University A
Incentives to promote compliance	"…But also, there has been little incentives for insiders to try…" "…I have seen my colleagues having no reason to do anything un-towards in the course of working since the working conditions are already fulfilling…"	Informant 1: ICT Staff-University A
Investment in robust systems and people's capacity	"…we have not had major incidents of information security breach because we not only have a very well equipped and knowledgeable IT department who understands what needs to be done, but also a very respectable and compliant society if I may refer to staff and students alike. We have policies in place, and everyone abides by them…."	Informant 1: ICT Staff-University A
Involvement of the users of the policies	"…We have a process. Remember we are ISO certified, one of the key principles is the people involved so …."	Informant 2: ICT-Staff University B

Theoretical Code: Organizational Strategies		
Selective Code	Cited quote	Informant Mapping
Sensitization initiatives (Awareness)	"…there is an aspect of sensitization when changing. Well unless it is an emergency, I think policy takes a while [before] they get approved so that process from developing and getting them approved and there is a part of sensitization…."	Informant 2: ICT-Staff University B
Regulated access to only what the user needs (Control)	"…all information about our graduate that undergoes the university and our culture is that we provide access to our systems, to our ICT infrastructure, we provide access that is limited to what is required strictly enough to what is required if you need more it has to be requested and has to be justified…."	Informant 2: ICT-Staff University B
Least privilege access, Trust, and role-based access (Control)	"…You get the least privilege as possible to enable you to do your work. That is how usually we do it in our culture. Also, we have a culture of trust, but trust is based on roles. For example, if you are in charge of the database then we entrust you with everything, but within that we may have a DBA admin model via a DB system admin so there is that responsibility of passing some extra eye to another person, acting as checks and balances…."	Informant 2: ICT-Staff University B
Robust separation process to safeguard institution on malicious sabotage incidents	"…error but due to backup, we can always restore. Internally, we have not had cases of sabotage as such because also when for example, we are careful with staff when they are leaving, the exit processes safeguard us…."	Informant 2: ICT-Staff University B

Theoretical Code: Organizational Strategies		
Selective Code	Cited quote	Informant Mapping
Training on information security as one way of enhancing information security compliance (Controls)	"…The security section that deals now strictly with one of the things to enact is that they have been undertaking a lot of training on security and they are also implementing international standards in terms of framework insecurity some of them look very theoretical but here when they now put in ISO as a process then they become serious because they are audited as certain parameters…."	Informant 2: ICT-Staff University B
Internal incidents also prompt the initiatives to review existing policies and strengthen any loopholes that may exist	"…occasionally there will be some new development like a loophole has been discovered we move quickly to review…."	Informant 2: ICT-Staff University B
Internal learning initiatives	"…we try then to also talk to staff and students, we can conduct surveys and interviews, there are several methods that we use, and then from that, we also do some literature review and examining…."	Informant 3: Management level ICT-Staff -University B

Theoretical Code: Management Support		
Selective Code	Cited quote	Informant Mapping
Top management support with financing, awareness training resources, and field support, etc. Management ready to adopt SOPs and policies	"…It starts from ICT director here, he drives the process, then he is also in charge of updating top management periodically on policy compliance issues relating to ICT, and the top management, the way they support us is by providing, whenever we request for training related to security and any other ICT field, they support by offering/giving the facilities or the financial services that we require to go for these training…."	Informant 3: Management level ICT-Staff -University B
Evidence of periodic review of the information security policies	"…We have our security policies revised every year and at times when there is no special need to change it, we just maybe put a date when we reviewed it in terms of compliance, we wouldn't feel in the first initial stages, because people take some time to understand. But we also face challenges in that people don't read the policy, especially with the young. Though maturity is subjective, and it is more pronounced in those who can reason well with the policy in place…."	Informant 4: Management level ICT-Staff-University A
Management ready to support and adopt documented incidents and policies	"…So, in terms of compliance, the issue comes up when maybe something has been violated. That is when people will ask, ". Who said that...!" we say it is in the policy, you only have to read the document and you will get it? Now then we have it resolved and since it is	Informant 4: Management level ICT-Staff-University A

Theoretical Code: Management Support		
Selective Code	Cited quote	Informant Mapping
	documented and accepted by the university council and the managing board, they just must absorb it….”	
Evidence of management support	“…The support of management is at different levels. It starts from the ICT director here, he drives the process, then he is also in charge of updating top management periodically on policy compliance issues relating to ICT….”	Informant 3: Management level ICT-Staff -University B
Evidence of strategy to enhance information security policy management through KPIs	“…Those SOPs, once the management has absorbed and accepted it, everybody has to follow that, if it one is in breach of that, you will get the full force of that. And, even in our KPIs, revising these policies is part of it. And we always come up with a new policy as we go, and on a need basis because security is always changing. The kind of attacks that we used to get before are not the same ones….”	Informant 4: Management level ICT-Staff-University A
The independence of the ICT department is guaranteed. The ICT department is well funded	“…Management is very keen on ICT because the way ICT works here, much as it is a department in central administration is more or less an independent entity which is funded, and it has a budget….”	Informant 2: ICT-Staff University B
A dedicated information security management structure always creates a solution to handle information security challenges	“…And part of that budget goes to NIS Networks Infrastructure and Security. So, we have a budget for that. We present our budget based on the plans we have in terms of security to the management and most of the time we get	Informant 2: ICT-Staff University B

Theoretical Code: Management Support		
Selective Code	Cited quote	Informant Mapping
	the right budget to go and implement, where it is not possible, we asked for alternatives. When it is completely not possible, we go for a quick fix as we look for a permanent solution….”	
Evidence of leading by example from the top management	“…Even the VC himself does not exclusive rights to the PC. He cannot come and install anything without consulting the helpdesk. Even a Dean, cannot log in and install anything. That is how we get support. And if a dean insists that, that must be authorized by the highest levels and they have to prove why they have to install something that is not within the university policy….”	Informant 4: Management level ICT-Staff-University A
Management leading by example	“…I see my superiors are also very keen on following guidelines which if you ask me, is a positive gesture from top management. I believe that this is one thing that also encourages others in the lower sections be it staff or students to comply with whichever policies are in place. We have a strong culture in the university, and this is beyond just the information security policies….”	Informant 13: Non-ICT Staff – University A
Evidence of management support at different levels	“…The support of management is at different levels. It starts from the ICT director here, he drives the process, then he is also in charge of updating top management periodically on policy compliance issues relating to ICT, and the top	Informant 3: Management level ICT-Staff -University B

Theoretical Code: Management Support		
Selective Code	Cited quote	Informant Mapping
	management, the way they support us is by providing, whenever we request for training related to security and any other ICT field, they support by offering/giving the facilities or the financial services that we require to go for these training….”	
Management support	“…With regards to the management, I am not in a position to say much because I am only staff with limited access to interactions with management, but what I can say is that I have had a feeling that the IT staff has a lot of support for their work from the management. This is key to succeeding in what we want to achieve collectively as IT staff….”	Informant 7: ICT-Staff - University A
Management Support	“…With the support, we have made sure that stronger and robust contributions are made towards awareness creation and Campaigns ….”	Informant 17: Technical Staff – University B

Theoretical Code: External Organizational Factors		
Selective Code	Cited quote	Informant Mapping
ISO certification standard requirements drive part of the initiatives to review information security policies	"…We do review them on an annual basis because we also update our ISO in terms of our processes…."	Informant 2: ICT-Staff University B
National requirements by Government also provides a reason for information security policy renewals	"…but occasionally, we do reviews on-demand based on like govt based on what is happening…."	Informant 2: ICT-Staff University B
External incidents also prompt the initiatives to review existing policies and strengthen any loopholes that may exist	"…occasionally there will be some new development like a loophole has been discovered we move quickly to review …."	Informant 2: ICT-Staff University B
External regulations such as the ICT Authority and Communication Authority also influence how and when the information security policies are reviewed.	"…and again, we are regulated we have the ICT CA guidelines on administration server and all that. When the govt pushes you to comply, you must change and comply…."	Informant 2: ICT-Staff University B
Compliance at the institution level and membership level is partly shaped by the authority from external forces	"…We are a govt institution so we are under the ICT authority that we must adopt immediately…."	Informant 2: ICT-Staff University B
Annual auditing of the institution by external and Internal entities on conformity to the processes the institution has set aside	"…basically, they look at conformity and if there is any non-conformity that is reported, then we must work on them. So, we are checked on an annual basis externally and semi-annual basis internally…."	Informant 2: ICT-Staff University B
Learning best practices from peers	"…Besides, we also believe as an institution that learning from best practice help strengthen our initiatives. Why would we reinvent the wheel when it works somewhere already? …."	Informant 17: Technical Staff – University B

Theoretical Code: External Organizational Factors		
Selective Code	Cited quote	Informant Mapping
Learning best practices from peers	"…we identify a list of documents that we think would be important in impacting the process from the constitution to specific standards concerning ICT that are given by the ICT Authority and then other international standards, for example, ISO standards on Information Security…."	Informant 3: Management level ICT-Staff -University B
Learning from peers	"…we select a few which we consider saying top universities where we want to go then we also look at the current trends as regards cybersecurity…."	Informant 3: Management level ICT-Staff -University B

Theoretical Code: Policy Compliance Culture		
Selective Code	Cited quote	Informant Mapping
Few incidents of breaches	"…Fairly speaking, we have not had major incidents of information security breach because we not only have a very well equipped and knowledgeable IT department who understands what needs to be done…."	Informant 1: ICT Staff-University A
Confirmation of compliance with information security policies	"…we not only have a very well equipped and knowledgeable IT department who understands what needs to be done, but also a very respectable and compliant society if I may refer to staff and students alike. We have policies in place, and everyone abides by them…."	Informant 1: ICT Staff-University A
Not many issues arising on policy violations but just a few occasions	"…We have not had serious cases internal or maybe someone going against the policy and probably acting against our security measures, but we have once in a while we had had issues of carelessness, someone does something costly, an example is that we use a database in a different section where one is given access to develop and does an update that wipes and messes the systems due to human error but due to backup, we can always restore…."	Informant 2: ICT-Staff University B
Some form of compliance culture	"…Speaking from my own experience, I have been in the institution for more than 10 years working in a different section, my experience has drawn me to the view that we	Informant 13-Non-ICT Staff

Theoretical Code: Policy Compliance Culture		
Selective Code	Cited quote	Informant Mapping
	have a strong culture of complying with policies….”	
Information security compliance Cultural maturity	“…We also have a population that knows what it means to do the right thing. That means that every new person joining us finds a culture of securing our information assets….” “…I would say the culture in our University has matured in that for all the years we have been operating as an IT department, we have seen many challenges and found equally very robust ways of addressing them. We have managed to create an environment that makes it easy for our colleagues and students to work seamlessly with ICT infrastructure and software with minimal security risks. An easy ICT platform to use creates a safer acceptance. And this means that those who use ICT to perform their day to day tasks do not have a reason to compromise on security. As such I can say we are satisfied that the compliance culture in our institution has grown much….”	Informant 1: ICT Staff-University A
	“…I can describe our culture where we provide, we are in education, there is a lot of information that we safeguard, the academic resources, all information about our graduate that undergoes the university and our culture is that we provide access to our	Informant 2: ICT-Staff University B

Theoretical Code: Policy Compliance Culture		
Selective Code	Cited quote	Informant Mapping
	systems, to our ICT infrastructure, we provide access that is limited to what is required strictly enough to what is required if you need more it has to be requested and has to be justified. That is our culture. You get the least privilege as possible to enable you to do your work. That is how usually we do it in our culture. Also, we have a culture of trust, but trust is based on roles. For example, if you oversee the database then we entrust you with everything….”	
Information security compliance culture	“…I have noticed that indeed we have a cultural practice here at the university. What I cannot say for sure if the aspect of culture is in sync with what you can refer to as information security compliance….”	Informant 6: ICT-Student-University B
Compliance culture?	“…I believe that culture plays a very important role in shaping other cultures in any society. When I came in for the first time, I noticed that the students and staff had some form of way of life that was well established. I had no choice, but to conform. The university has several ways of nurturing the new members to feel part of the community. As you have observed, if you walk around, you will realize that no one walks on the grass to create short cut routes. Everyone is conscious of what the colleague will see or say about them. And I believe that	Informant 7: ICT-Staff - University A

Theoretical Code: Policy Compliance Culture		
Selective Code	Cited quote	Informant Mapping
	this is what creates an element of compliance with information security policies as well in the university….”	
Elements of Culture	“…I believe that I have seen some form of cultural roots. As a student, I have seen many initiatives to inculcate cultural values among the students and staff of the universities. That is a good thing because, despite our former environment, when we get here as either student or staff, we are bound by the values. Of course, you will always find a few rebellious students or what I can call those who don’t care, but all in all, culture is a big thing in the university….”	Informant 9: Student – University A
Positive indication of a culture of compliance	“…What am happy about is the fact that the university authority has been very impactful in creating awareness of the risks. This has made even those who would be violating the policies unconsciously to be on the right side. And even though I may not be able to fully confirm this, I believe that there is a positive culture of information security compliance….”	Informant 12: Non-ICT student - University B
Strong compliance culture	“…Speaking from my own experience, I have been in the institution for more than 10 years working in a different section, my experience has drawn me to the view that we have a strong culture of complying with policies. I see my superiors are also very	Informant 13: Non-ICT Staff – University A

Theoretical Code: Policy Compliance Culture		
Selective Code	Cited quote	Informant Mapping
	keen on following guidelines which if you ask me, is a positive gesture from top management. I believe that this is one thing that also encourages others in the lower sections be it staff or students to comply with whichever policies are in place. We have a strong culture in the university, and this is beyond just the information security policies. We are a certified institution through the ISO certification and as such, I believe that part of the reasons to qualify is the aspect of a strong culture of compliance with international standards which are contributed largely by the staff and students. So, culture, if you ask me, is much stronger in terms of individual and institutional compliance….”	
information security culture	"…I believe we have a culture as a university. The culture, especially around the information system related to culture can be seen in how the management and the student handle issues related to policies. Our university, and by that I would like to restrict myself to the campus, has done a great job in creating awareness….”	Informant 14: Non-ICT Student – University B
Information security compliance culture	"…I believe there is some information security culture. We do get occasionally alerts of potential risks in our emails from the ICT office. This helps us prepare. When I came in as a student 3 years ago, I	Informant 15: Non-ICT Student – University A

Theoretical Code: Policy Compliance Culture		
Selective Code	Cited quote	Informant Mapping
	was bombarded with a lot of information about information systems policy. And I think this is a good this. You know, if the students and staff have such kind of information, then one has no reason to go against it….”	
A semblance of compliance culture	“…We have an established culture in the university that enables us to comply with policies. I know of efforts that have been made for new and old members to feel that they are part of the university community. When you walk into the university, you will notice that the way staff and students alike carry themselves speaks of a culture that speaks of respect to the norms and values. For example, did you notice how students and staff obey simple regulations such as presenting their identifications when accessing the buildings? That is what I call a simple culture of compliance….”	Informant 16: Staff (Non-IT) University A
Information Security culture with the support of the management	“…However, to efforts that we make are deeply dependent also on how management supports us. This has been the best ingredient for our successful information security culture. With support, we have made sure that stronger and robust contributions are made towards awareness creation and campaigns. We have seen several responses from the students and faculty as well as non-teaching staff who use the	Informant 17: Technical Staff – University B

Theoretical Code: Policy Compliance Culture		
Selective Code	Cited quote	Informant Mapping
	university’s ICT assets who have asked queries. This shows us that everyone is interested to be part of the culture….”	
There is cultural maturity	“…In terms of security, as I had said, I have no idea what cybersecurity is, but I have always seen emails alerting us about being careful with clicking links anyhow in our inbox. I guess those in charge of our internet are aware of these possibilities. So, I would say there is some form of monitoring. This is a good thing since it shows a system that works on that front. We are a mature culture, and management is always at the front leading by example. This one I can attest to myself as a staff with many years in this university….”	Informant 18: Non-Technical Staff – University A
Acknowledgment of compliance culture	"...there is a culture of compliance, but as you have already heard, some restrictions are just too much, and we have to find a way out. It is not right, but what do we do…."	Informant 19: Student University B
Some feeling of cultural presence	“…All I can say is that I believe we have an embedded culture as a university. This, I can say is drawn from the history that this university has since I started knowing it while I was young. However, concerning information security culture, I am not sure whether to say there is a strong culture or not. I can only speculate that there is one	Informant 20: Student University B

Theoretical Code: Policy Compliance Culture		
Selective Code	Cited quote	Informant Mapping
	because of not so many reports on compromises….”	

APPENDIX 9: Selective Coding Stage

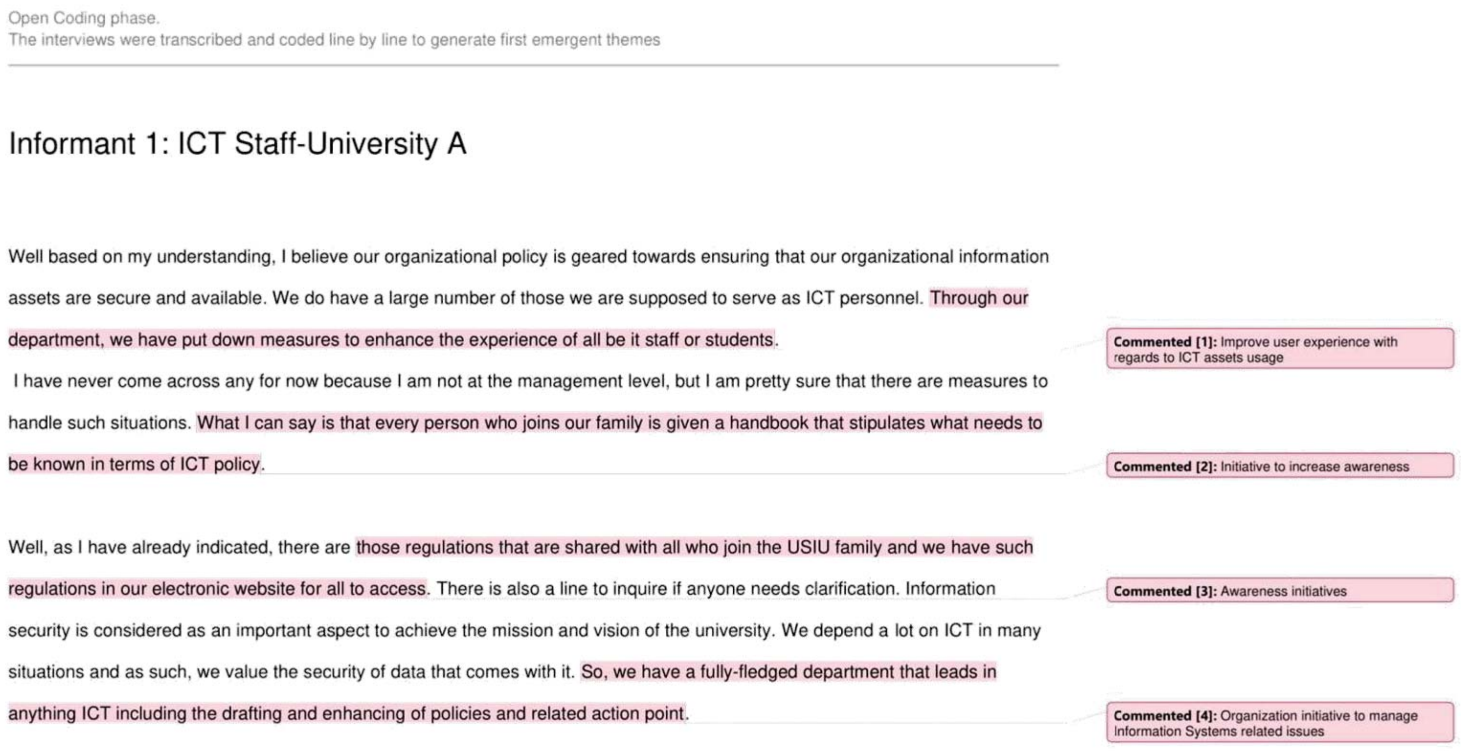
Emergent Themes (Axial Coding)	Grouped Themes (Selective Coding)
• Improve user experience with regards to ICT assets usage • Initiative to increase awareness • Awareness initiatives • Organization initiative to manage information systems related issues • Incidents of breaches not pronounced • Possibilities of procedures to handle breaches • Punishments of breach actions • Incentives to promote compliance • Improvement of working conditions as incentives • Few incidents of breaches • Investment in robust systems and people's capacity • Belief in students' and staffs' ability to follow and do what is required • Confirmation of compliance with information security policies • Organizational initiative to improve awareness • Inducting new members of the team to the awareness initiatives • Established ease of access • Cultural maturity • Maturity in handling information security challenges • Systems to make working with information security policies assets easy • Technology acceptance initiatives • With the ease of using ICT assets, and making ISPs accessible and easy to understand, compliance has also been on the positive trend • Compliance culture is greater • Regular updates of information security policies • Involvement of the users of the policies • Sensitization initiatives • Independence of the ICT department is guaranteed • The ICT department is well funded • A dedicated information security management structure always creates a solution to handle information security challenges • Regulated access to only what the user needs • Least privilege access • Trust and role-based access • Process documentation	Group 1 Age factor, Social upbringing, Educational background Social pressure, Group 2 Regulatory authorities, ISO certification and standards, Best practices from peers Group 3 Awareness program, Capacity development, Control mechanisms, Robust tracking and incident flagging processes, Deterrent initiatives Group 4 Perceived ease of ISP application, Perceived risks of ISP application Individual attitude

• Service provision chatter, like a Service Level Agreement (SLA) within the institution • This ensures that everyone knows how and when to expect a service delivery • An external factor that enhances compliance within the organization • There is a system to report any non-conformity with the laid down procedures and processes • Working based on trust among the employees • Trust is built over time based on an acting capacity basis in which a background check is done in the process • Not many issues arising on policy violations but just a few occasions • only careless incidents have been experienced • Data backup and restoration systems in place • Robust separation process to safeguard institution on malicious sabotage incidents • Training on information security as one way of enhancing information security compliance • Enacting international standards in terms of a framework on information security that are audit-able • Fewer concerns with staff in terms of breaches Apart from few malicious actions • Audit processes to catch breaches in time • Actions are taken by making the one who has breached to lose the job • A case of a tamper-proof and system with an audit trail to deter the would-be staff to cause the breach of data • Safeguards for password protection enhances some form of compliance with a control mechanism • Evidence of information security policy review mechanism • The mechanism to enhance compliance with information security policies • External factor considerations to enhance compliance strategy • Current trends in information security management • Stakeholder consultations internally • Identification of best practice to strategize on information security compliance • The revised policy is an inclusive document that has undergone a thorough and systemic drafting process • Continued monitoring and evaluating the level of compliance, (organizational vigilance)	Group 5 , Group 6: statements supporting the establishment of information security compliance culture Management support, Few breaches of information security policy, Culture of taking responsibility as managers, Management leading by example

• Evidence of management support at different levels • Process driving stage and support from the top directorate • Continued keeping the top management up to date on compliance issue, • Top management support with financing, awareness training resources, and field support, etc. • Identification of the role played by the human component of information security • System to address the human component that can lead to non-compliant behavior or incidents • Awareness and capacity-building strategies • Receptive stakeholders due to the training and capacity building • Affirmative response on the role awareness and training has on overall compliance with information security policies • Measures targeting the demographic aspect of information security compliance • Initiatives to make it easier to create awareness • Ease of improving how awareness tools are implemented • Several policy tools for the members • Accountability tools to enforce compliance with information security policies • A few cases of breaches, but actions have been taken to handle them • Incident reporting strategy to help provide lessons learned and best practices platform • Evidence of periodic review of the information security policies • Management ready to support and adopt documented incidents and policies • Few internal information security breach incidents • Ways to educate and create awareness initiatives • Awareness initiatives • Management ready to adopt SOPs and policies • Evidence of management support • Evidence of strategy to enhance information security policy management through KPIs • Evidence of leading by example from the top management • Awareness initiatives • Systems processes and controls to avert any occurrences before they happen • Systems to give access on a need to do basis	

• Processes and controls how data is accessed • There is a big problem of resolving the social pressure that we have had to struggle with. Many students do some things because it is the trend, and it impacts heavily on our efforts as information security managers to enhance compliance • Systems in place to monitor the network and how and who is using it • Deterrence controls • Ability to trace and violator • Systems to enhance accountability to who uses the networks and ICT assets • Sensitization and awareness programs • Challenges handling the younger generation in the institution • Also, ways of managing the senior members like staff • Training is important	

APPENDIX 10: Open Coding Stage



Open Coding phase.
The interviews were transcribed and coded line by line to generate first emergent themes

Informant 1: ICT Staff-University A

Well based on my understanding, I believe our organizational policy is geared towards ensuring that our organizational information assets are secure and available. We do have a large number of those we are supposed to serve as ICT personnel. Through our department, we have put down measures to enhance the experience of all be it staff or students.

Commented [1]: Improve user experience with regards to ICT assets usage

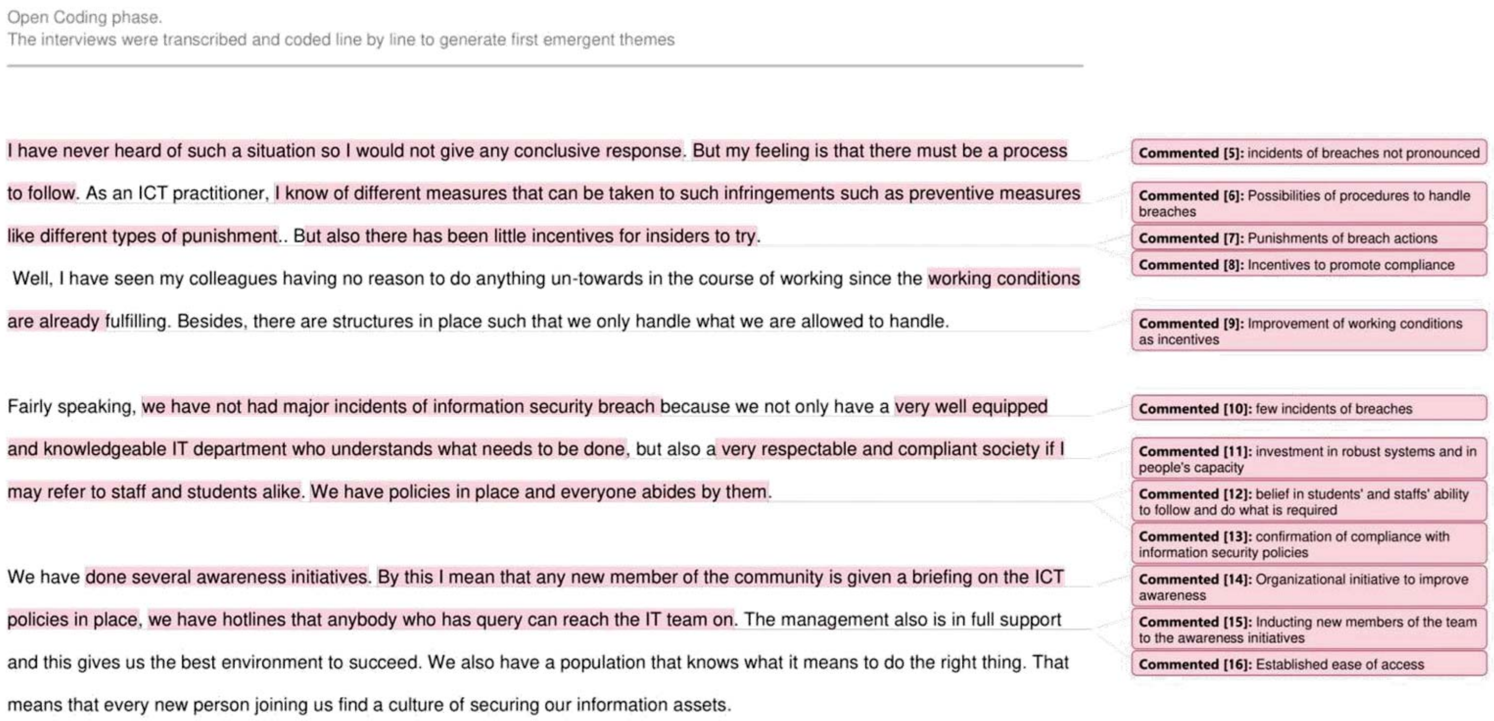
I have never come across any for now because I am not at the management level, but I am pretty sure that there are measures to handle such situations. What I can say is that every person who joins our family is given a handbook that stipulates what needs to be known in terms of ICT policy.

Commented [2]: Initiative to increase awareness

Well, as I have already indicated, there are those regulations that are shared with all who join the USIU family and we have such regulations in our electronic website for all to access. There is also a line to inquire if anyone needs clarification. Information security is considered as an important aspect to achieve the mission and vision of the university. We depend a lot on ICT in many situations and as such, we value the security of data that comes with it. So, we have a fully-fledged department that leads in anything ICT including the drafting and enhancing of policies and related action point.

Commented [3]: Awareness initiatives

Commented [4]: Organization initiative to manage Information Systems related issues



Open Coding phase.
The interviews were transcribed and coded line by line to generate first emergent themes

I have never heard of such a situation so I would not give any conclusive response. But my feeling is that there must be a process to follow. As an ICT practitioner, I know of different measures that can be taken to such infringements such as preventive measures like different types of punishment.. But also there has been little incentives for insiders to try.

Well, I have seen my colleagues having no reason to do anything un-towards in the course of working since the working conditions are already fulfilling. Besides, there are structures in place such that we only handle what we are allowed to handle.

Fairly speaking, we have not had major incidents of information security breach because we not only have a very well equipped and knowledgeable IT department who understands what needs to be done, but also a very respectable and compliant society if I may refer to staff and students alike. We have policies in place and everyone abides by them.

We have done several awareness initiatives. By this I mean that any new member of the community is given a briefing on the ICT policies in place, we have hotlines that anybody who has query can reach the IT team on. The management also is in full support and this gives us the best environment to succeed. We also have a population that knows what it means to do the right thing. That means that every new person joining us find a culture of securing our information assets.

Commented [5]: incidents of breaches not pronounced

Commented [6]: Possibilities of procedures to handle breaches

Commented [7]: Punishments of breach actions

Commented [8]: Incentives to promote compliance

Commented [9]: Improvement of working conditions as incentives

Commented [10]: few incidents of breaches

Commented [11]: investment in robust systems and in people's capacity

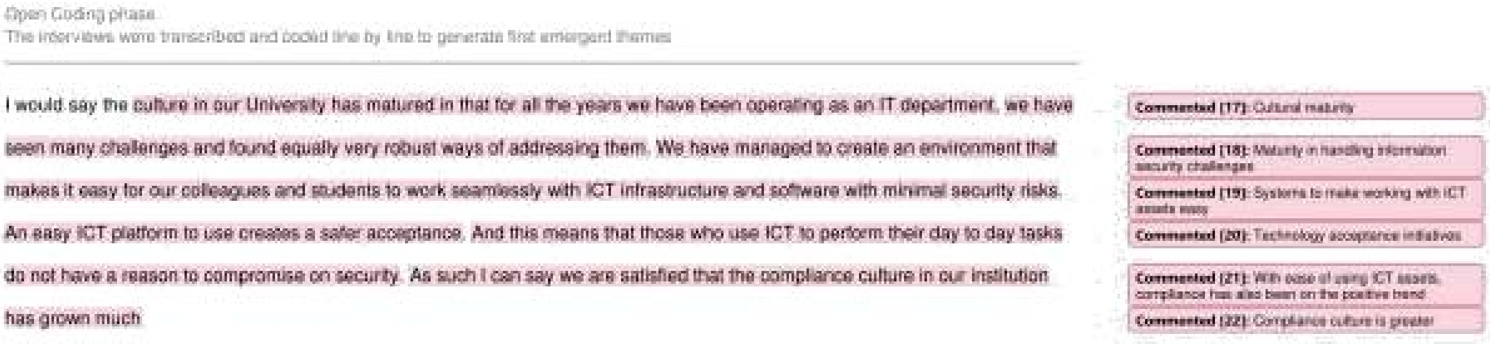
Commented [12]: belief in students' and staffs' ability to follow and do what is required

Commented [13]: confirmation of compliance with information security policies

Commented [14]: Organizational initiative to improve awareness

Commented [15]: Inducting new members of the team to the awareness initiatives

Commented [16]: Established ease of access



Open Coding phase

The interviews were transcribed and coded line by line to generate first emergent themes

I would say the culture in our University has matured in that for all the years we have been operating as an IT department, we have seen many challenges and found equally very robust ways of addressing them. We have managed to create an environment that makes it easy for our colleagues and students to work seamlessly with ICT infrastructure and software with minimal security risks. An easy ICT platform to use creates a safer acceptance. And this means that those who use ICT to perform their day to day tasks do not have a reason to compromise on security. As such I can say we are satisfied that the compliance culture in our institution has grown much

Commented [17]: Cultural maturity

Commented [18]: Maturity in handling information security challenges

Commented [19]: Systems to make working with ICT assets easy

Commented [20]: Technology acceptance initiatives

Commented [21]: With ease of using ICT assets, compliance has also been on the positive trend

Commented [22]: Compliance culture is greater

Informant 2: ICT-Staff University B

We do review them on an annual basis because we also update our ISO in terms of our processes but once in a while, we do reviews on demand based on like govt based on what is happening, once in a while there will be some new development like a loophole has been discovered we move quickly to review and again we are regulated we have the ICT CA guidelines on administration server and all that. when the govt pushes you to comply, you have to change and comply. We are a govt institution so we are under the ICT authority that we must adopt immediately.

We have process. Remember we are ISO certified, one of the key principles is the people involvement so there is an aspect of sensitization when changing. Well unless it is an emergency I think policy takes a while [before] they get approved so that process from developing and getting them approved and also there is a part of sensitization.

Management is very keen on ICT because the way ICT works here, much as it is a department in central administration is more of less an independent entity which is funded and it has a budget. And part of that budget goes to NIS Networks Infrastructure and Security. So, we have a

Commented [23]: Regular updates of information security policies

Commented [24]: ISO certification standard requirements drives part of the initiatives to review information security policies

Commented [25]: National requirements by Government also provides a reason for information security policy renewals

Commented [26]: Internal and external incidents also prompt the initiatives to review existing policies and strengthen any loopholes that may exist

Commented [27]: External regulations such as ICT authority and Communication Authority also influences how and when the information security policies are reviewed.

Commented [28]: Compliance at the institution level and at membership level is partly shaped by the authority from external forces

Commented [29]: Involvement of the users of the policies

Commented [30]: Sensitization initiatives

Commented [31]: Independence of the ICT department is guaranteed

Commented [32]: The ICT department is well funded

Commented [33]: Dedicated information security management structure budget for that. We present our budget based on the plans we have in terms of security to the management and most of the time we get the right budget to go and implement, where it is not possible, we asked for alternatives. When it is completely not possible, we go for quick fix as we look for a permanent solution.

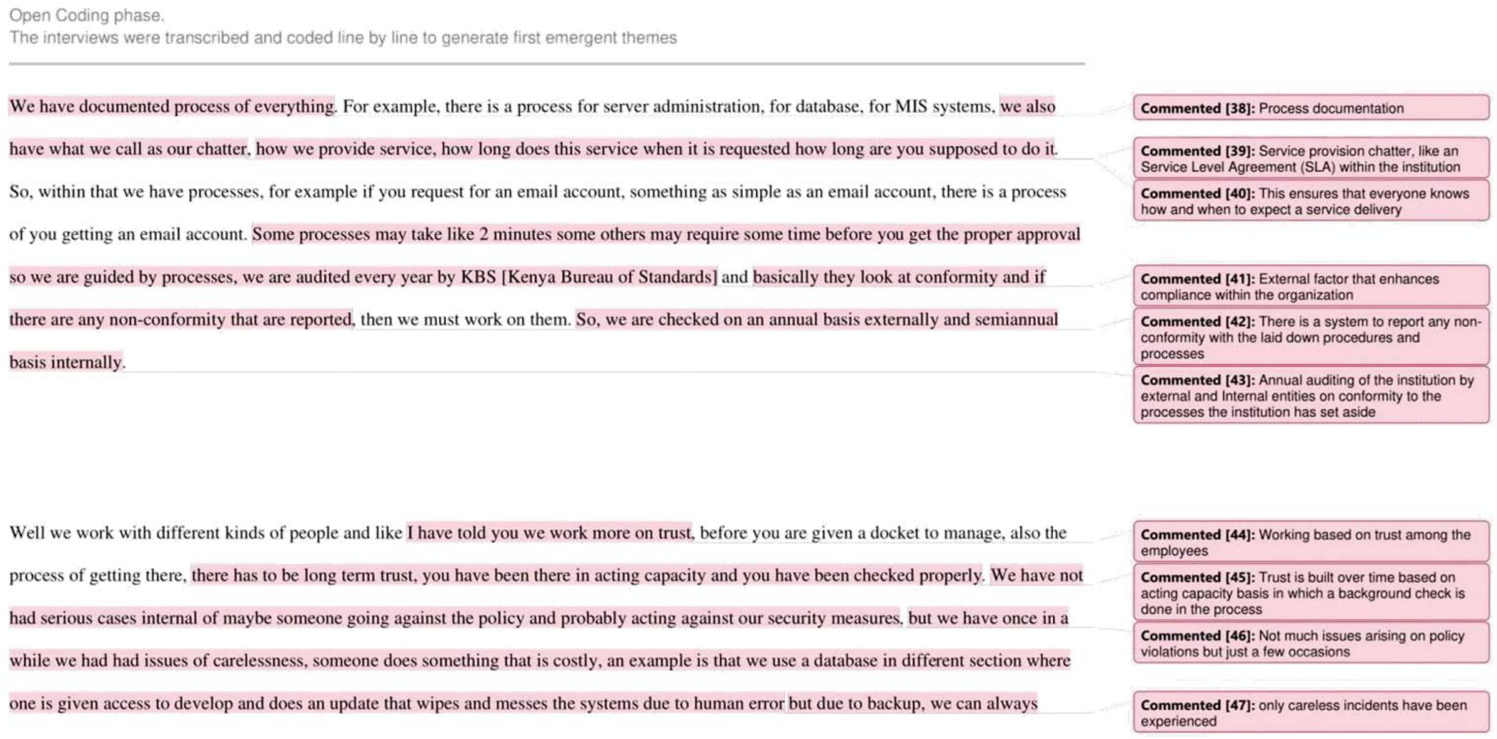
Commented [34]: always creates a solution to handle information security challenges

I can describe our culture where we provide, we are in education, there is a lot of information that we safeguard, the academic resources, all information about our graduate that undergoes the university and our culture is that we provide access to our systems, to our ICT infrastructure, we provide access that is limited to what is required strictly enough to what is required if you need more it has to be requested and has to be justified. that is our culture. You get the least privilege as possible to enable you do your work. That is how usually we do it in our culture. Also, we have a culture of trust but trust based on roles. For example, if you are in charge of the database then we entrust you with everything, but within that we may have a DBA admin model via a DB system admin so there is that responsibility of passing some extra eye to another person, **[acting like...]** checks and balances

Commented [35]: Regulated access to only what the user needs

Commented [36]: Trust and role-based access

Commented [37]: Peer to peer checks and balances. Everyone knows someone is watching



Open Coding phase.
The interviews were transcribed and coded line by line to generate first emergent themes

We have documented process of everything. For example, there is a process for server administration, for database, for MIS systems, we also have what we call as our chatter, how we provide service, how long does this service when it is requested how long are you supposed to do it. So, within that we have processes, for example if you request for an email account, something as simple as an email account, there is a process of you getting an email account. Some processes may take like 2 minutes some others may require some time before you get the proper approval so we are guided by processes, we are audited every year by KBS [Kenya Bureau of Standards] and basically they look at conformity and if there are any non-conformity that are reported, then we must work on them. So, we are checked on an annual basis externally and semiannual basis internally.

Commented [38]: Process documentation

Commented [39]: Service provision chatter, like an Service Level Agreement (SLA) within the institution

Commented [40]: This ensures that everyone knows how and when to expect a service delivery

Commented [41]: External factor that enhances compliance within the organization

Commented [42]: There is a system to report any non-conformity with the laid down procedures and processes

Commented [43]: Annual auditing of the institution by external and Internal entities on conformity to the processes the institution has set aside

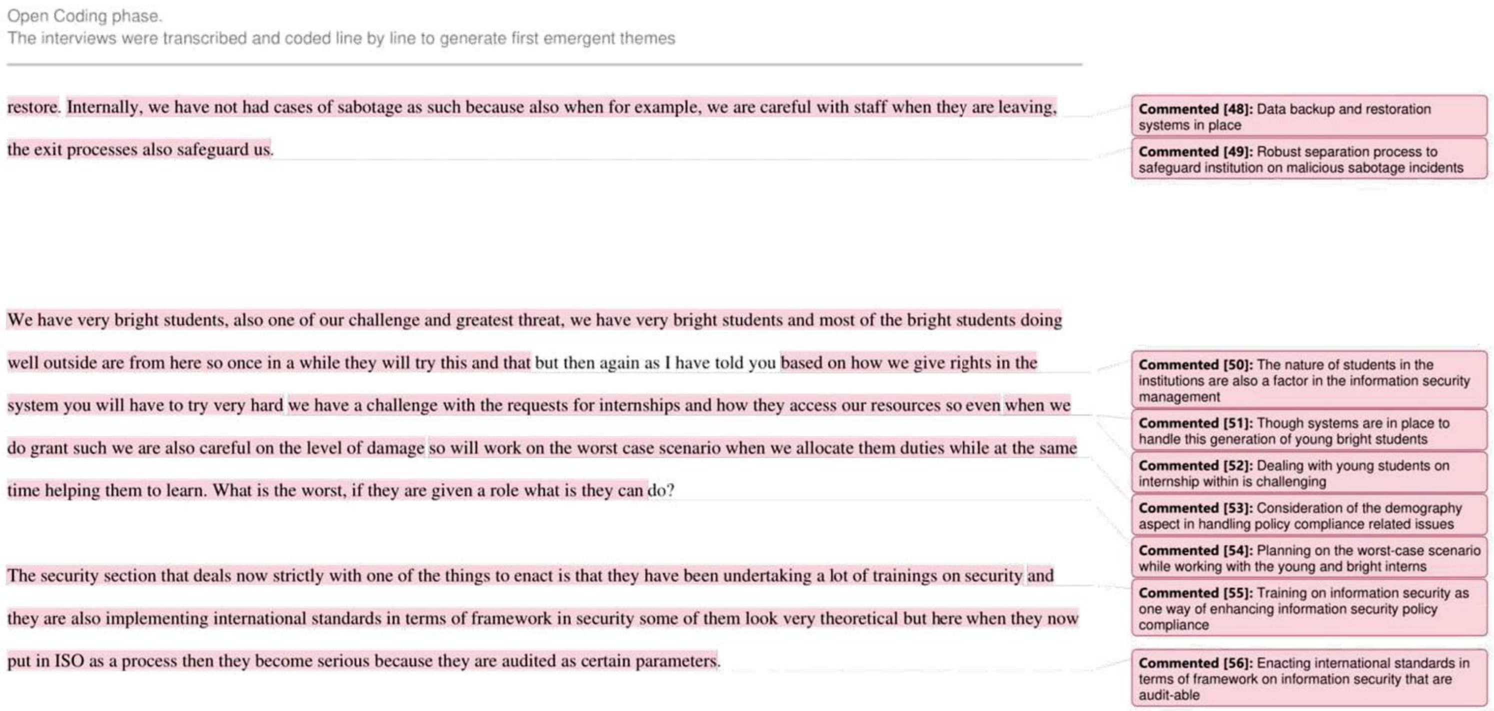
Well we work with different kinds of people and like I have told you we work more on trust, before you are given a docket to manage, also the process of getting there, there has to be long term trust, you have been there in acting capacity and you have been checked properly. We have not had serious cases internal of maybe someone going against the policy and probably acting against our security measures, but we have once in a while we had had issues of carelessness, someone does something that is costly, an example is that we use a database in different section where one is given access to develop and does an update that wipes and messes the systems due to human error but due to backup, we can always

Commented [44]: Working based on trust among the employees

Commented [45]: Trust is built over time based on acting capacity basis in which a background check is done in the process

Commented [46]: Not much issues arising on policy violations but just a few occasions

Commented [47]: only careless incidents have been experienced



Open Coding phase.
The interviews were transcribed and coded line by line to generate first emergent themes

restore. Internally, we have not had cases of sabotage as such because also when for example, we are careful with staff when they are leaving, the exit processes also safeguard us.

Commented [48]: Data backup and restoration systems in place

Commented [49]: Robust separation process to safeguard institution on malicious sabotage incidents

We have very bright students, also one of our challenge and greatest threat, we have very bright students and most of the bright students doing well outside are from here so once in a while they will try this and that but then again as I have told you based on how we give rights in the system you will have to try very hard we have a challenge with the requests for internships and how they access our resources so even when we do grant such we are also careful on the level of damage so will work on the worst case scenario when we allocate them duties while at the same time helping them to learn. What is the worst, if they are given a role what is they can do?

Commented [50]: The nature of students in the institutions are also a factor in the information security management

Commented [51]: Though systems are in place to handle this generation of young bright students

Commented [52]: Dealing with young students on internship within is challenging

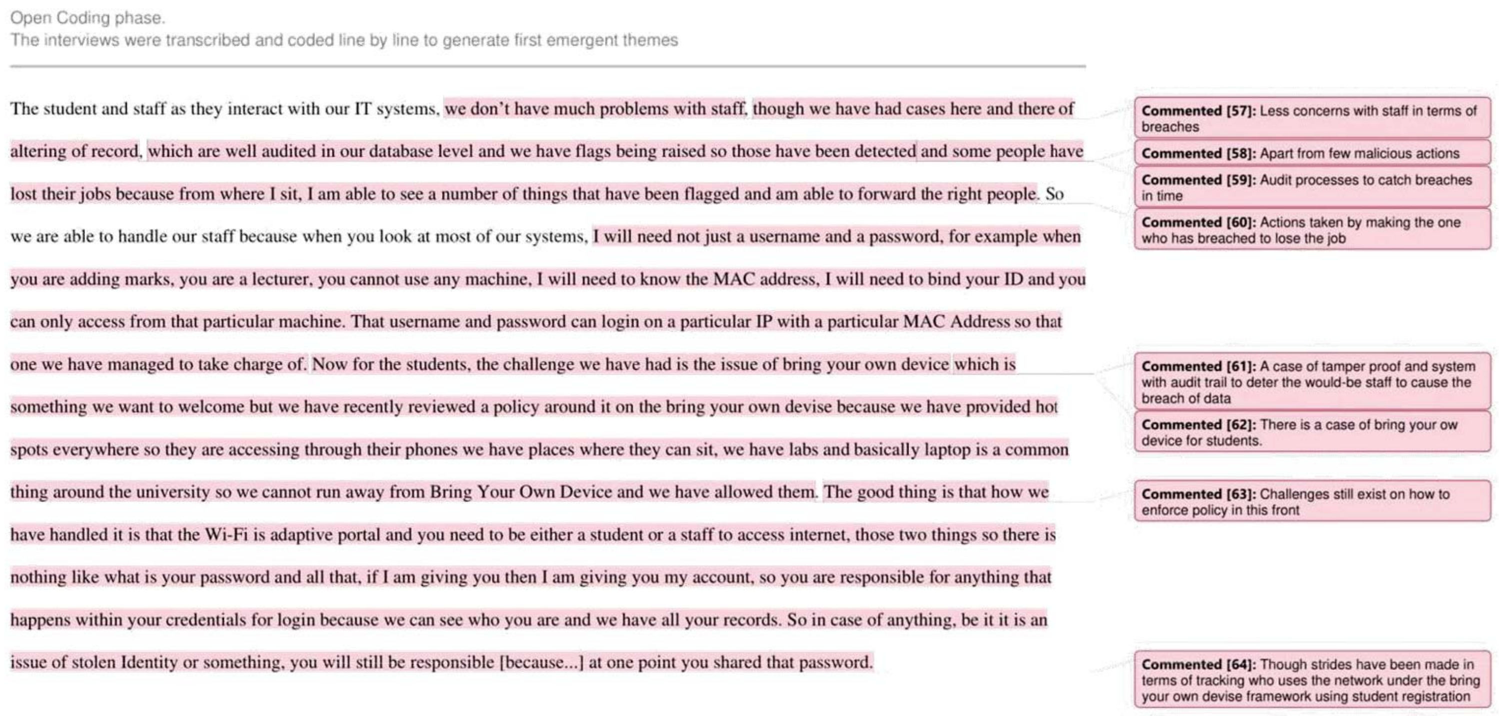
Commented [53]: Consideration of the demography aspect in handling policy compliance related issues

Commented [54]: Planning on the worst-case scenario while working with the young and bright interns

The security section that deals now strictly with one of the things to enact is that they have been undertaking a lot of trainings on security and they are also implementing international standards in terms of framework in security some of them look very theoretical but here when they now put in ISO as a process then they become serious because they are audited as certain parameters.

Commented [55]: Training on information security as one way of enhancing information security policy compliance

Commented [56]: Enacting international standards in terms of framework on information security that are audit-able



Open Coding phase.
The interviews were transcribed and coded line by line to generate first emergent themes

The student and staff as they interact with our IT systems, we don’t have much problems with staff, though we have had cases here and there of altering of record, which are well audited in our database level and we have flags being raised so those have been detected and some people have lost their jobs because from where I sit, I am able to see a number of things that have been flagged and am able to forward the right people. So we are able to handle our staff because when you look at most of our systems, I will need not just a username and a password, for example when you are adding marks, you are a lecturer, you cannot use any machine, I will need to know the MAC address, I will need to bind your ID and you can only access from that particular machine. That username and password can login on a particular IP with a particular MAC Address so that one we have managed to take charge of. Now for the students, the challenge we have had is the issue of bring your own device which is something we want to welcome but we have recently reviewed a policy around it on the bring your own devise because we have provided hot spots everywhere so they are accessing through their phones we have places where they can sit, we have labs and basically laptop is a common thing around the university so we cannot run away from Bring Your Own Device and we have allowed them. The good thing is that how we have handled it is that the Wi-Fi is adaptive portal and you need to be either a student or a staff to access internet, those two things so there is nothing like what is your password and all that, if I am giving you then I am giving you my account, so you are responsible for anything that happens within your credentials for login because we can see who you are and we have all your records. So in case of anything, be it it is an issue of stolen Identity or something, you will still be responsible [because...] at one point you shared that password.

Commented [57]: Less concerns with staff in terms of breaches

Commented [58]: Apart from few malicious actions

Commented [59]: Audit processes to catch breaches in time

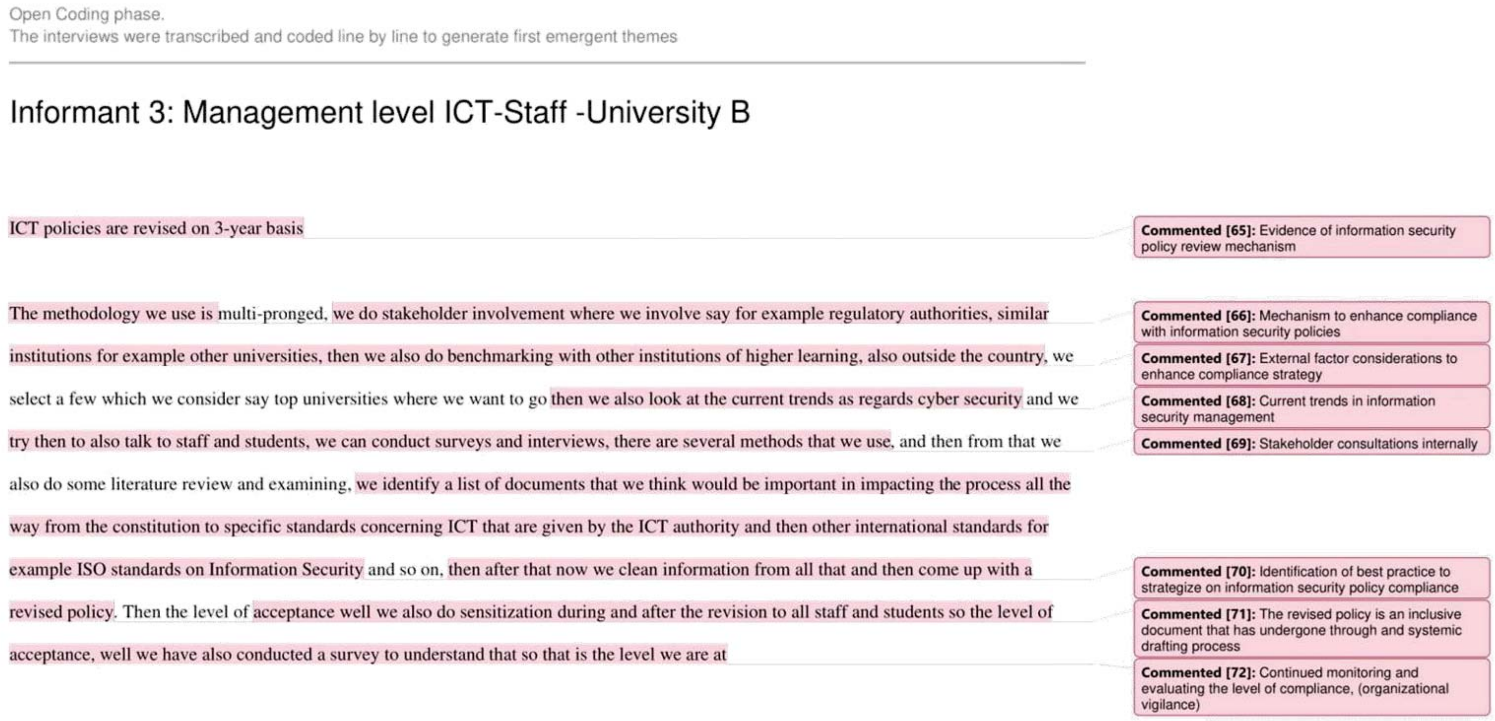
Commented [60]: Actions taken by making the one who has breached to lose the job

Commented [61]: A case of tamper proof and system with audit trail to deter the would-be staff to cause the breach of data

Commented [62]: There is a case of bring your ow device for students.

Commented [63]: Challenges still exist on how to enforce policy in this front

Commented [64]: Though strides have been made in terms of tracking who uses the network under the bring your own devise framework using student registration



Open Coding phase.
The interviews were transcribed and coded line by line to generate first emergent themes

Informant 3: Management level ICT-Staff -University B

ICT policies are revised on 3-year basis

The methodology we use is multi-pronged, we do stakeholder involvement where we involve say for example regulatory authorities, similar institutions for example other universities, then we also do benchmarking with other institutions of higher learning, also outside the country, we select a few which we consider say top universities where we want to go then we also look at the current trends as regards cyber security and we try then to also talk to staff and students, we can conduct surveys and interviews, there are several methods that we use, and then from that we also do some literature review and examining, we identify a list of documents that we think would be important in impacting the process all the way from the constitution to specific standards concerning ICT that are given by the ICT authority and then other international standards for example ISO standards on Information Security and so on, then after that now we clean information from all that and then come up with a revised policy. Then the level of acceptance well we also do sensitization during and after the revision to all staff and students so the level of acceptance, well we have also conducted a survey to understand that so that is the level we are at

Commented [65]: Evidence of information security policy review mechanism

Commented [66]: Mechanism to enhance compliance with information security policies

Commented [67]: External factor considerations to enhance compliance strategy

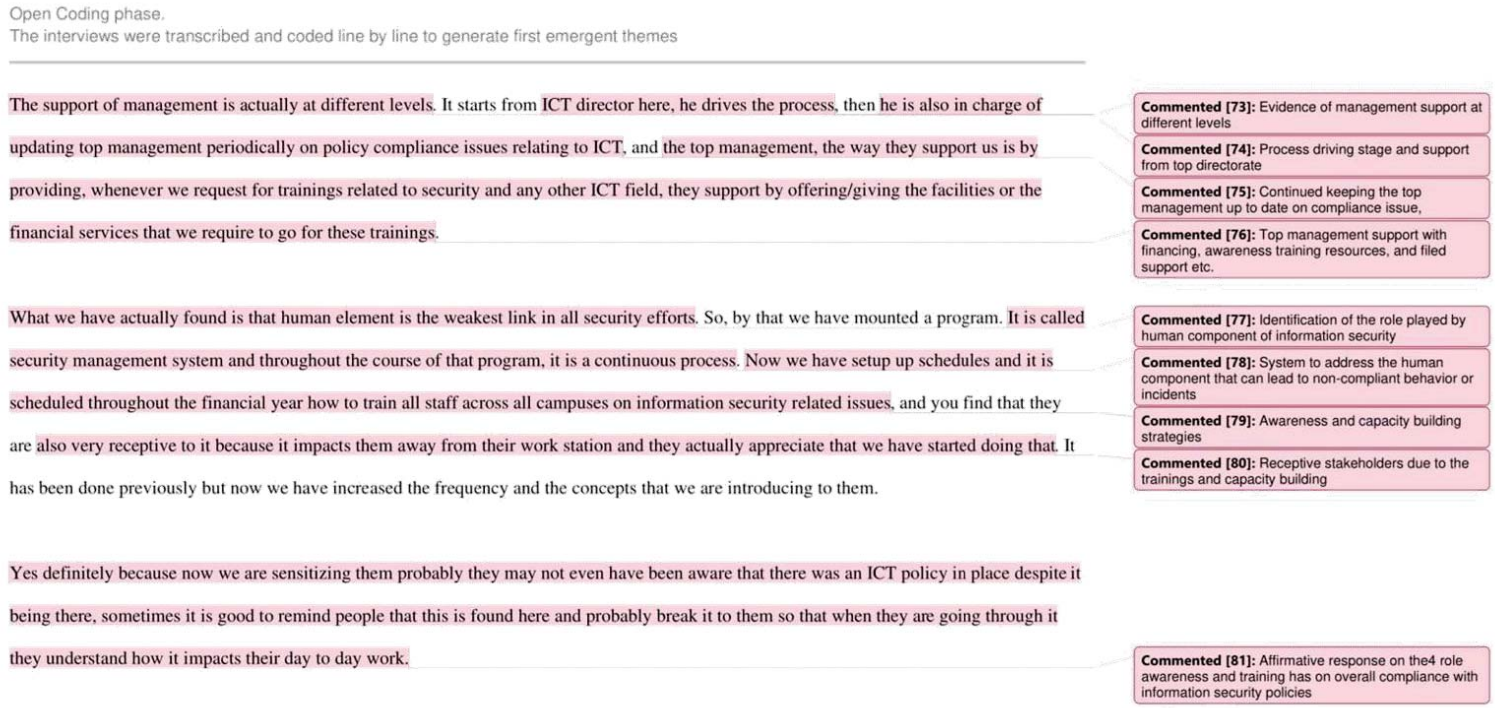
Commented [68]: Current trends in information security management

Commented [69]: Stakeholder consultations internally

Commented [70]: Identification of best practice to strategize on information security policy compliance

Commented [71]: The revised policy is an inclusive document that has undergone through and systemic drafting process

Commented [72]: Continued monitoring and evaluating the level of compliance, (organizational vigilance)



Open Coding phase.
The interviews were transcribed and coded line by line to generate first emergent themes

The support of management is actually at different levels. It starts from ICT director here, he drives the process, then he is also in charge of updating top management periodically on policy compliance issues relating to ICT, and the top management, the way they support us is by providing, whenever we request for trainings related to security and any other ICT field, they support by offering/giving the facilities or the financial services that we require to go for these trainings.

What we have actually found is that human element is the weakest link in all security efforts. So, by that we have mounted a program. It is called security management system and throughout the course of that program, it is a continuous process. Now we have setup up schedules and it is scheduled throughout the financial year how to train all staff across all campuses on information security related issues, and you find that they are also very receptive to it because it impacts them away from their work station and they actually appreciate that we have started doing that. It has been done previously but now we have increased the frequency and the concepts that we are introducing to them.

Yes definitely because now we are sensitizing them probably they may not even have been aware that there was an ICT policy in place despite it being there, sometimes it is good to remind people that this is found here and probably break it to them so that when they are going through it they understand how it impacts their day to day work.

Commented [73]: Evidence of management support at different levels

Commented [74]: Process driving stage and support from top directorate

Commented [75]: Continued keeping the top management up to date on compliance issue,

Commented [76]: Top management support with financing, awareness training resources, and filed support etc.

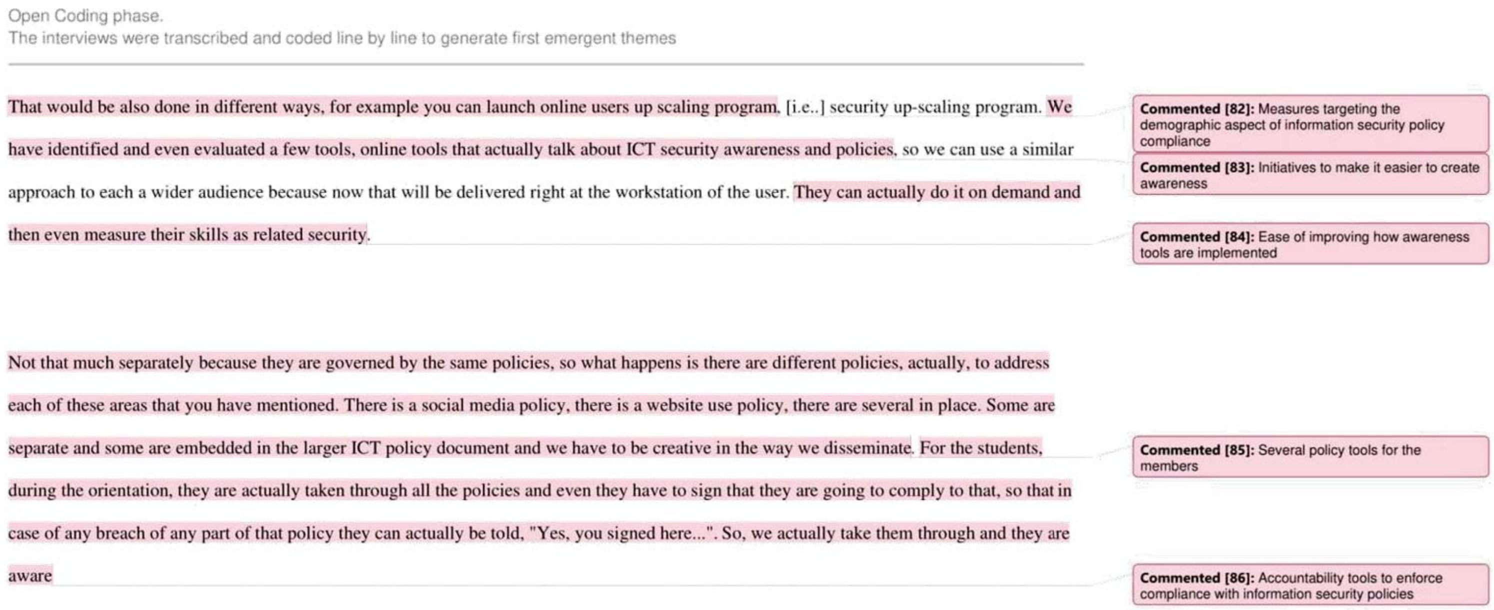
Commented [77]: Identification of the role played by human component of information security

Commented [78]: System to address the human component that can lead to non-compliant behavior or incidents

Commented [79]: Awareness and capacity building strategies

Commented [80]: Receptive stakeholders due to the trainings and capacity building

Commented [81]: Affirmative response on the4 role awareness and training has on overall compliance with information security policies



Open Coding phase.
The interviews were transcribed and coded line by line to generate first emergent themes

That would be also done in different ways, for example you can launch online users up scaling program, [i.e..] security up-scaling program. We have identified and even evaluated a few tools, online tools that actually talk about ICT security awareness and policies, so we can use a similar approach to each a wider audience because now that will be delivered right at the workstation of the user. They can actually do it on demand and then even measure their skills as related security.

Commented [82]: Measures targeting the demographic aspect of information security policy compliance

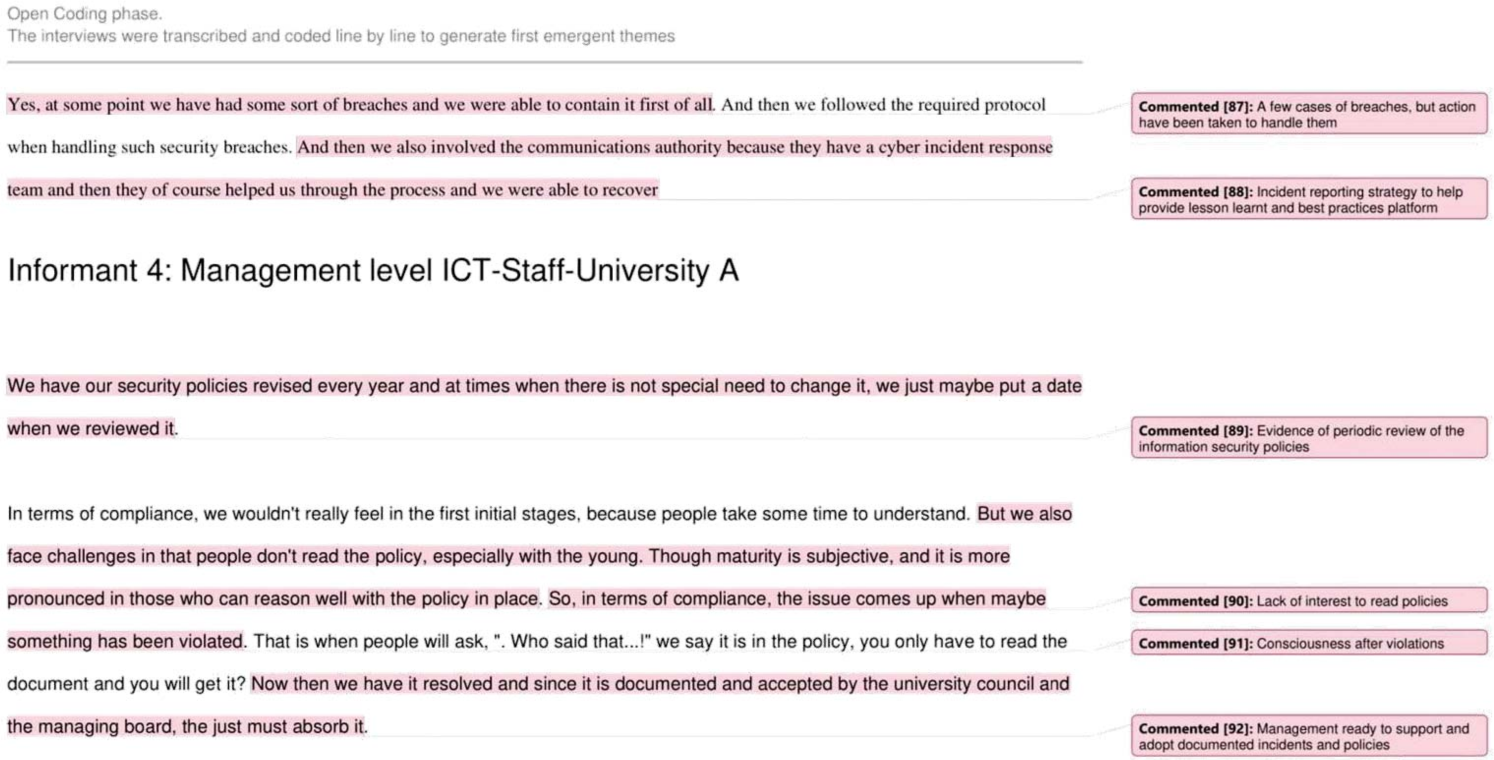
Commented [83]: Initiatives to make it easier to create awareness

Commented [84]: Ease of improving how awareness tools are implemented

Not that much separately because they are governed by the same policies, so what happens is there are different policies, actually, to address each of these areas that you have mentioned. There is a social media policy, there is a website use policy, there are several in place. Some are separate and some are embedded in the larger ICT policy document and we have to be creative in the way we disseminate. For the students, during the orientation, they are actually taken through all the policies and even they have to sign that they are going to comply to that, so that in case of any breach of any part of that policy they can actually be told, "Yes, you signed here...". So, we actually take them through and they are aware

Commented [85]: Several policy tools for the members

Commented [86]: Accountability tools to enforce compliance with information security policies



Open Coding phase.
The interviews were transcribed and coded line by line to generate first emergent themes

Yes, at some point we have had some sort of breaches and we were able to contain it first of all. And then we followed the required protocol when handling such security breaches. And then we also involved the communications authority because they have a cyber incident response team and then they of course helped us through the process and we were able to recover

Commented [87]: A few cases of breaches, but action have been taken to handle them

Commented [88]: Incident reporting strategy to help provide lesson learnt and best practices platform

Informant 4: Management level ICT-Staff-University A

We have our security policies revised every year and at times when there is not special need to change it, we just maybe put a date when we reviewed it.

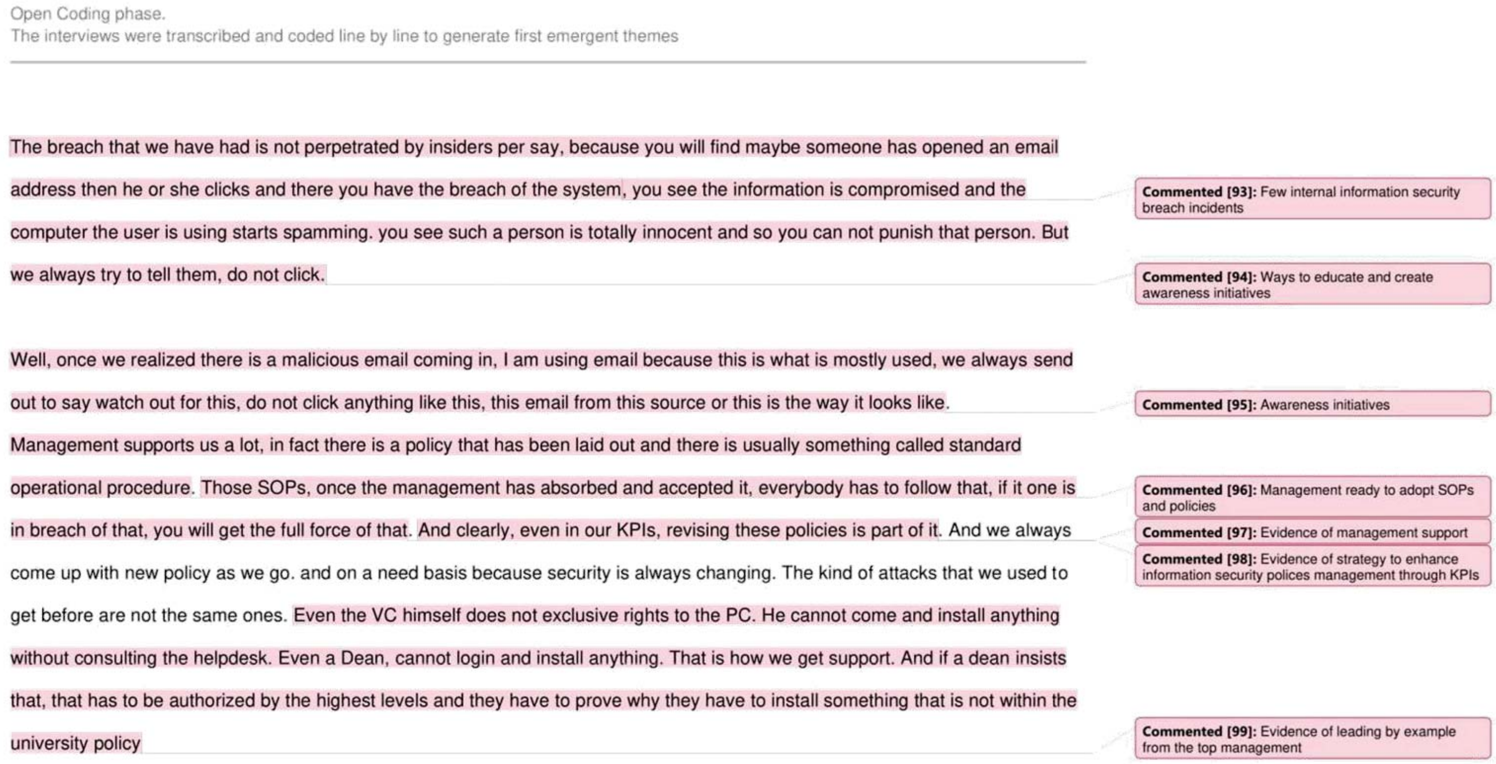
Commented [89]: Evidence of periodic review of the information security policies

In terms of compliance, we wouldn't really feel in the first initial stages, because people take some time to understand. But we also face challenges in that people don't read the policy, especially with the young. Though maturity is subjective, and it is more pronounced in those who can reason well with the policy in place. So, in terms of compliance, the issue comes up when maybe something has been violated. That is when people will ask, ". Who said that...!" we say it is in the policy, you only have to read the document and you will get it? Now then we have it resolved and since it is documented and accepted by the university council and the managing board, the just must absorb it.

Commented [90]: Lack of interest to read policies

Commented [91]: Consciousness after violations

Commented [92]: Management ready to support and adopt documented incidents and policies



Open Coding phase.
The interviews were transcribed and coded line by line to generate first emergent themes

The breach that we have had is not perpetrated by insiders per say, because you will find maybe someone has opened an email address then he or she clicks and there you have the breach of the system, you see the information is compromised and the computer the user is using starts spamming. you see such a person is totally innocent and so you can not punish that person. But we always try to tell them, do not click.

Well, once we realized there is a malicious email coming in, I am using email because this is what is mostly used, we always send out to say watch out for this, do not click anything like this, this email from this source or this is the way it looks like. Management supports us a lot, in fact there is a policy that has been laid out and there is usually something called standard operational procedure. Those SOPs, once the management has absorbed and accepted it, everybody has to follow that, if it one is in breach of that, you will get the full force of that. And clearly, even in our KPIs, revising these policies is part of it. And we always come up with new policy as we go. and on a need basis because security is always changing. The kind of attacks that we used to get before are not the same ones. Even the VC himself does not exclusive rights to the PC. He cannot come and install anything without consulting the helpdesk. Even a Dean, cannot login and install anything. That is how we get support. And if a dean insists that, that has to be authorized by the highest levels and they have to prove why they have to install something that is not within the university policy

Commented [93]: Few internal information security breach incidents

Commented [94]: Ways to educate and create awareness initiatives

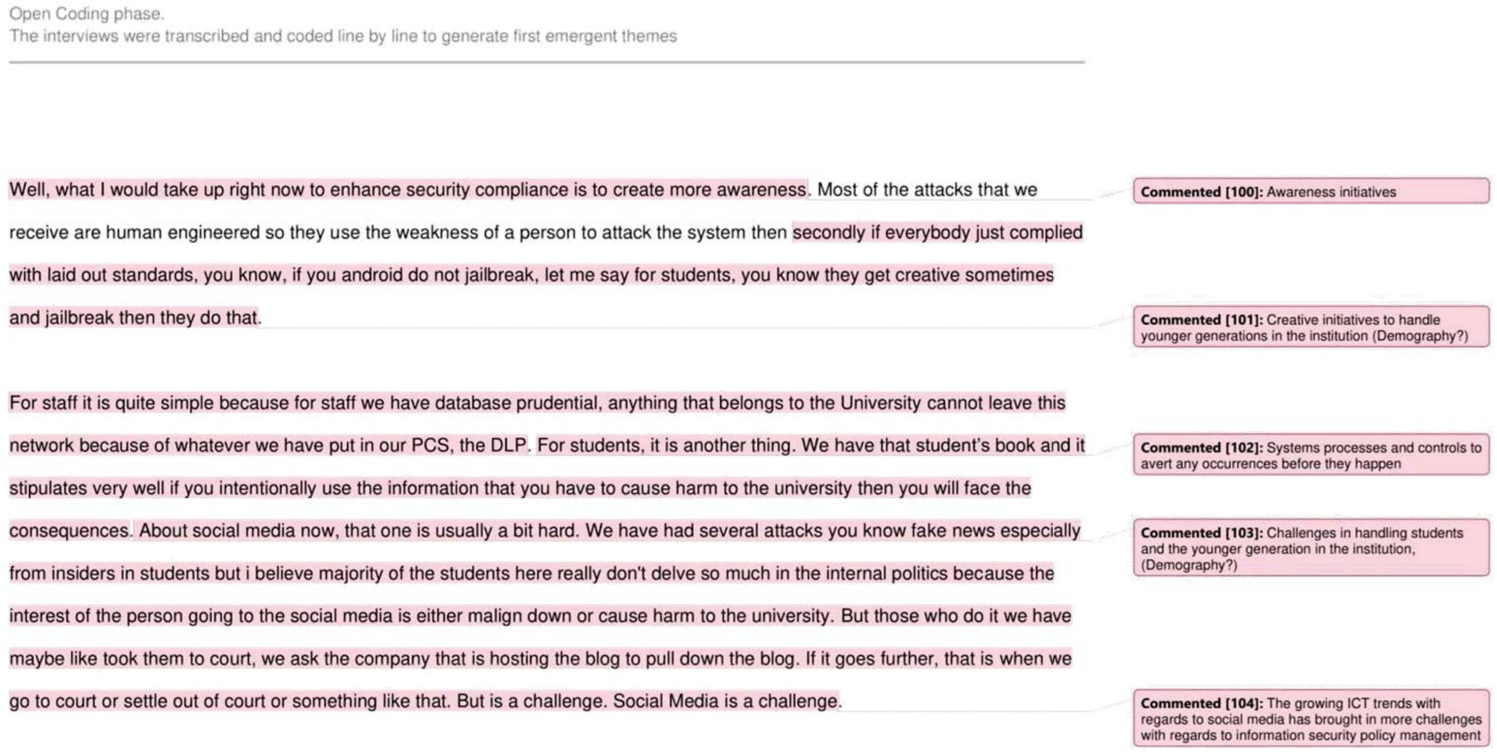
Commented [95]: Awareness initiatives

Commented [96]: Management ready to adopt SOPs and policies

Commented [97]: Evidence of management support

Commented [98]: Evidence of strategy to enhance information security polices management through KPIs

Commented [99]: Evidence of leading by example from the top management



Well, what I would take up right now to enhance security compliance is to create more awareness. Most of the attacks that we receive are human engineered so they use the weakness of a person to attack the system then secondly if everybody just complied with laid out standards, you know, if you android do not jailbreak, let me say for students, you know they get creative sometimes and jailbreak then they do that.

For staff it is quite simple because for staff we have database prudential, anything that belongs to the University cannot leave this network because of whatever we have put in our PCS, the DLP. For students, it is another thing. We have that student's book and it stipulates very well if you intentionally use the information that you have to cause harm to the university then you will face the consequences. About social media now, that one is usually a bit hard. We have had several attacks you know fake news especially from insiders in students but i believe majority of the students here really don't delve so much in the internal politics because the interest of the person going to the social media is either malign down or cause harm to the university. But those who do it we have maybe like took them to court, we ask the company that is hosting the blog to pull down the blog. If it goes further, that is when we go to court or settle out of court or something like that. But is a challenge. Social Media is a challenge.

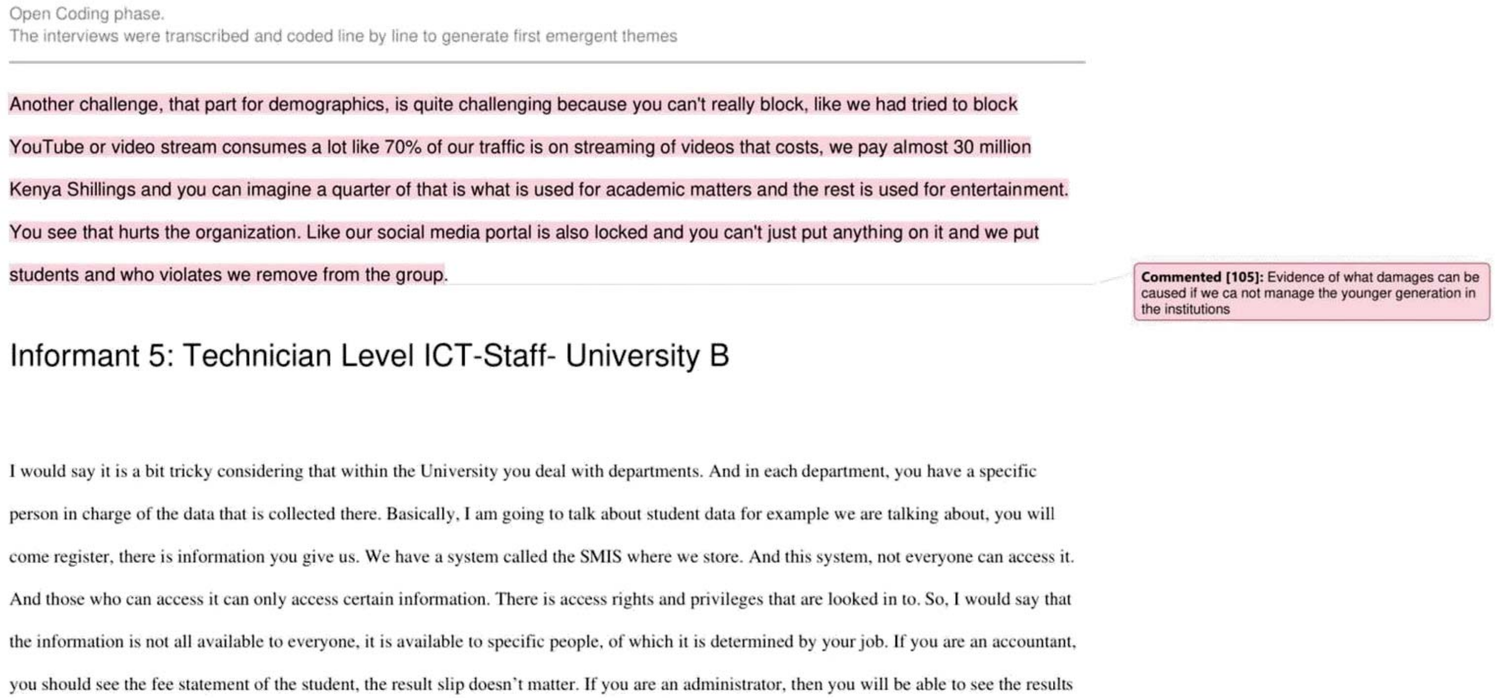
Commented [100]: Awareness initiatives

Commented [101]: Creative initiatives to handle younger generations in the institution (Demography?)

Commented [102]: Systems processes and controls to avert any occurrences before they happen

Commented [103]: Challenges in handling students and the younger generation in the institution, (Demography?)

Commented [104]: The growing ICT trends with regards to social media has brought in more challenges with regards to information security policy management



Another challenge, that part for demographics, is quite challenging because you can't really block, like we had tried to block YouTube or video stream consumes a lot like 70% of our traffic is on streaming of videos that costs, we pay almost 30 million Kenya Shillings and you can imagine a quarter of that is what is used for academic matters and the rest is used for entertainment. You see that hurts the organization. Like our social media portal is also locked and you can't just put anything on it and we put students and who violates we remove from the group.

Commented [105]: Evidence of what damages can be caused if we ca not manage the younger generation in the institutions

Informant 5: Technician Level ICT-Staff- University B

I would say it is a bit tricky considering that within the University you deal with departments. And in each department, you have a specific person in charge of the data that is collected there. Basically, I am going to talk about student data for example we are talking about, you will come register, there is information you give us. We have a system called the SMIS where we store. And this system, not everyone can access it. And those who can access it can only access certain information. There is access rights and privileges that are looked in to. So, I would say that the information is not all available to everyone, it is available to specific people, of which it is determined by your job. If you are an accountant, you should see the fee statement of the student, the result slip doesn't matter. If you are an administrator, then you will be able to see the results see the statement but you cannot alter the statement. So, I would say that when it comes to how we deal with the information we are very specific as to who deals with what information. So that there are very few people who would have all information.

Commented [106]: Systems to give access on a need to do basis

First of all, you cannot access the data outside the university, we are talking about those who manage SMIS which holds all the data of the students. For you to access it, then ICT will require to have your MAC address, and your IP address and then your payroll number so it is merged with this. So, if you are going home you will not be able to access it because you will be using a different machine. So, it means there is some control. If it is the results, you cannot have a pdf of it. If you need it you will have to do the hard-copy. Which brings in another aspect of printing where you print from a specific [printer], it is centralized in most departments. Also, it gives some control of data.

Commented [107]: Processes and controls to how data is accessed

Yes, we have restrictions and for example in the university even when you use the internet, you use your registration now with a password. So, it means that if you are doing anything fishy, we can be able to identify who is this. We have an ICT security who would follow up to find out, they would tell us in your lab someone trying to access this and this site. And they are doing something illegal. So, there is some controls even for the students. They cannot just access betting sites, vulgar sites because it would indicate, this is the registration number. So, I can come and say I may look for this person, it becomes easier to trace them. You will be blocked on the network such that a registration number cannot be used by any other person. And they are encouraged to be the only one using that username and password. The username is your registration

Commented [108]: Systems in place to monitor the network and how and who is using it

Commented [109]: Deterrence controls

Commented [110]: Ability to trace and violator number the password you can even create your own, there is one generated by the system but you can always create your own. So, if you give it out, it is at your own risk.

Commented [111]: Systems to enhance accountability to who uses the networks and ICT assets

What we do is that the people within the departments are supposed to sensitize especially the first years and tell them this is something that can even bring you to a point where you can be expelled. So, we start warning them from first year. We have had situations where we have had someone's registration number used for something, trying to hack another system, so we have examples of colleagues which you can which works very well because they know it is not a threat, it is something that is going to actually happen. If you give your registration to your relative, they come try something illegal, we will not defend you because we will just use the evidence, we have.

Commented [112]: Sensitization and awareness programs

Commented [113]: Everyone has to take responsibility if the violations have been traced to their credentials

I would say, when it comes to compliance, we have to look at it from two points of view. We have to look at it from the point of view of a student, and a staff. So a student, you have to make them aware because majority do not know the consequences of some of the things they do, especially when it comes to things to do with copyright, they will want to download a movie, store it in a machine in the lab, and then it can be accessed by others. They don't understand the copyright, they just hear there is something called copyright. They don't know what that is. Then now we have the staff. We have the lecturers, we have the technical staff, we have the administrative staff. Training is very important for them. Because you will find technical staff you just tell to students. There are two trainings here we can talk about. We have the technical and we have what we call customer care. We issue threats, but we do not tell them why. Am going to be telling you "Don't do this, don't do this..." why? The

Commented [114]: Challenges handling the younger generation in the institution

Commented [115]: Also, ways of managing the senior members like staff

Commented [116]: Training is important generation we have today deals with reason and not threat. You threaten them, you encourage them to do it. You tell theme this are the consequences of doing this. You bring it down to their level, especially like the ones of computer science that I am dealing with, I will tell them you are going to develop an application. How would you feel if someone hosted it online for free, now it makes them think. They put themselves in that situation and they see it wouldn't be fair to them, so why would I do it? for others? I think that is one way. Now the staff, they need to have a way of dealing with students. We have a very big problem because there is a communication breakdown. We come from a generation where we were told don't do this and you stop. They come from a generation where they are told if you do this, this is what is going to happen. so, you see there is a gap, big one.

Commented [117]: Generational handling techniques (Demography?)

Yes, if you interact with them you will even notice that to some extent, they teach the older generation a lot. These are people who have spent all their time in computers. The older generation only interacted with computers while working. So, there are things they wouldn't know but these young people because they spend all their time on the computer, they will know. If you interact with them from my experience, I have learnt a lot from them. I would sit down and they would tell me, you guys have blocked download of torrents, but my colleagues are still doing it, this is how they are doing it, and they show you. You get to realize that there is a backdoor. But without interacting with them you will just be wondering how comes, you go find a hard disk is full of movies, is full of books, where are they coming from. And we have blocked torrents. it is that they are able to identify the backdoor.

Commented [118]: Structured way of tackling the generational challenges (Demography?)

Actually what I have come to realize is that there are those students who we would call them notorious when it comes to the use of machines, they will change your password they will come, in most cases, if you sit down with those students, you will notice they have very small problems. They want to install a software, they have talked to the technician, he has refused because he does not understand what this software is for. So it is very easy to deal with them if you are going to sit down with them and understanding them and they will solve so many of your problems. Because when you talk to them, you get the picture they paint for you. You get to understand, oh, this is what they need because of this. But most of us we are older than them and we know, if it is programming you are going to use visual basic or python and that is it. Then they come and tell you a strange name and you are like; I have never heard of that. So, you dismiss them. While if you sat down and listen to them and found out, and they give you their reasons, you will be able to come to an agreement.

Commented [119]: Demographic challenges

Commented [120]: Demographic challenges

Commented [121]: Ways that have worked in handling the Demographic challenges

Informant 6: ICT-Student- University B

My take is that it is not a big deal for me when it comes to information security policy compliance. As an IT student, I am well aware of the issues around information security and cyber security. Many of my colleagues from other departments usually fall prey from scams that come in disguises. For example, a few days ago, we had an incident where a student mistakenly gave their access to a trusted friend and ended up being compromised because the access was the same one used for internet purposes. My advice to young people in the university is always not to trust even a friend. Because the password is what keeps you from trouble. I have not seen major issue of breaches at a personal level, and I cannot for

Commented [EO122]: Carelessness among some students certain tell if there has been any in the university. I have noticed that indeed we have a cultural practice here at the university. What I cannot say for sure if the aspect of culture is in sync with what you can refer to as information security policy compliance. I have seen many other students including those from IT related courses being very smart and able to bypass the policies. Some of my colleagues are very clever you know.

Commented [EO123]: Culture

Commented [EO124]: Education background influence

Informant 7: ICT-Staff - University A

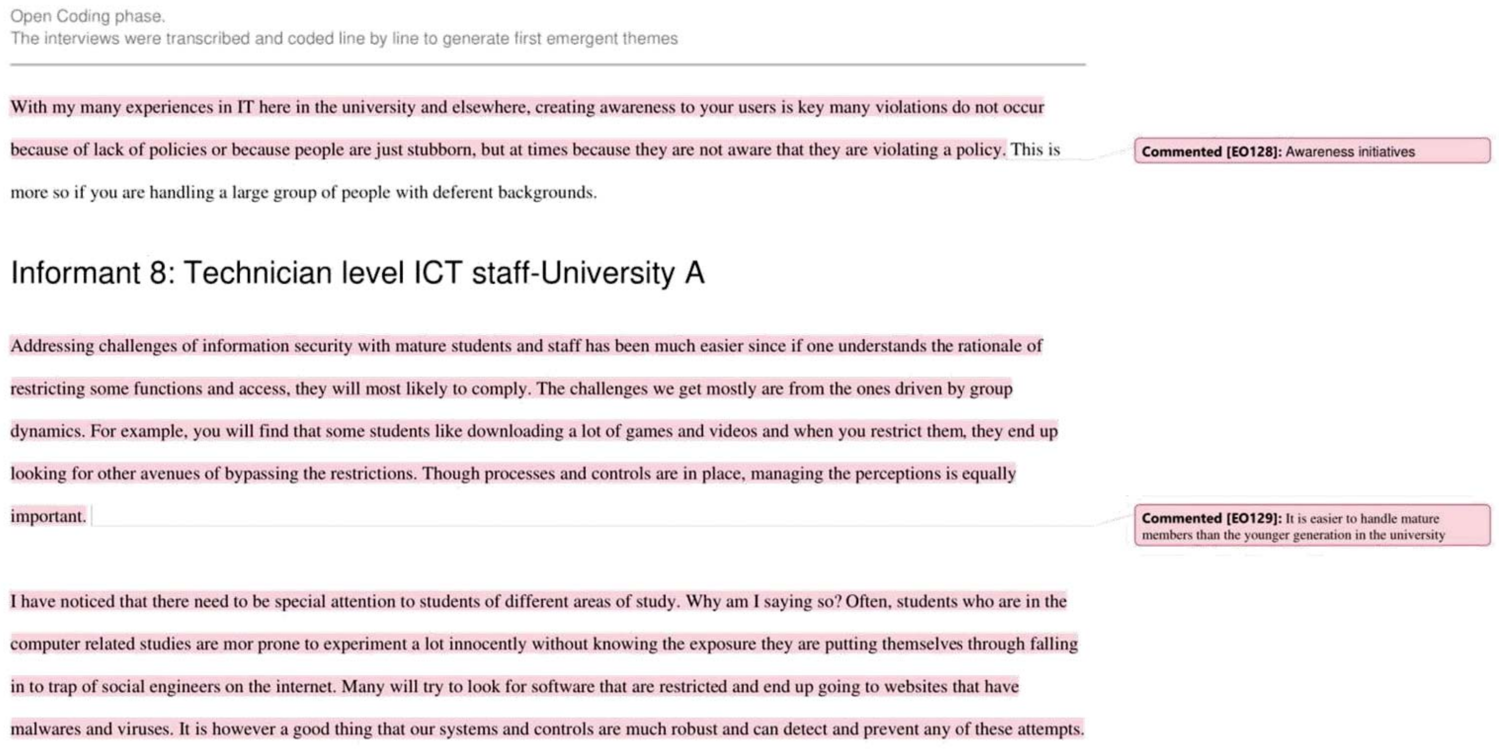
I believe that culture plays a very important role in shaping other cultures in any society. When I came in for the first time, I noticed that the students and staff had some form of way of life that was well established. I had no choice, but to conform. The university has several ways of nurturing the new members to feel part of the community. If you walk around, you will realize that no one walks on the grass to create short cut routes. Everyone is conscious of what the colleague will see or say about them. And I believe that this is what creates an element of compliance with information security policies as well in the university.

Commented [EO125]: Culture presence

Commented [EO126]: Compliance culture?

With regards to the management, I am not in a position to say much because I am only a staff with limited access to interactions with management, but what I can say is that I have had a feeling that the IT staff has a lot of support for their work from the management. This is key to succeeding in what we want to achieve collectively as IT staff.

Commented [EO127]: Management support



With my many experiences in IT here in the university and elsewhere, creating awareness to your users is key many violations do not occur because of lack of policies or because people are just stubborn, but at times because they are not aware that they are violating a policy. This is more so if you are handling a large group of people with deferent backgrounds.

Commented [EO128]: Awareness initiatives

Informant 8: Technician level ICT staff-University A

Addressing challenges of information security with mature students and staff has been much easier since if one understands the rationale of restricting some functions and access, they will most likely to comply. The challenges we get mostly are from the ones driven by group dynamics. For example, you will find that some students like downloading a lot of games and videos and when you restrict them, they end up looking for other avenues of bypassing the restrictions. Though processes and controls are in place, managing the perceptions is equally important.

Commented [EO129]: It is easier to handle mature members than the younger generation in the university

I have noticed that there need to be special attention to students of different areas of study. Why am I saying so? Often, students who are in the computer related studies are mor prone to experiment a lot innocently without knowing the exposure they are putting themselves through falling in to trap of social engineers on the internet. Many will try to look for software that are restricted and end up going to websites that have malwares and viruses. It is however a good thing that our systems and controls are much robust and can detect and prevent any of these attempts.

We have had cases where we have asked the students to communicate when they need something that can be useful in enhancing their studies. Students who are in the computer science are usually most likely to violate policies due to their needs. This is particularly so if they sneak in software that are not allowed. They also know how to crack a software as opposed to students in other discipline.

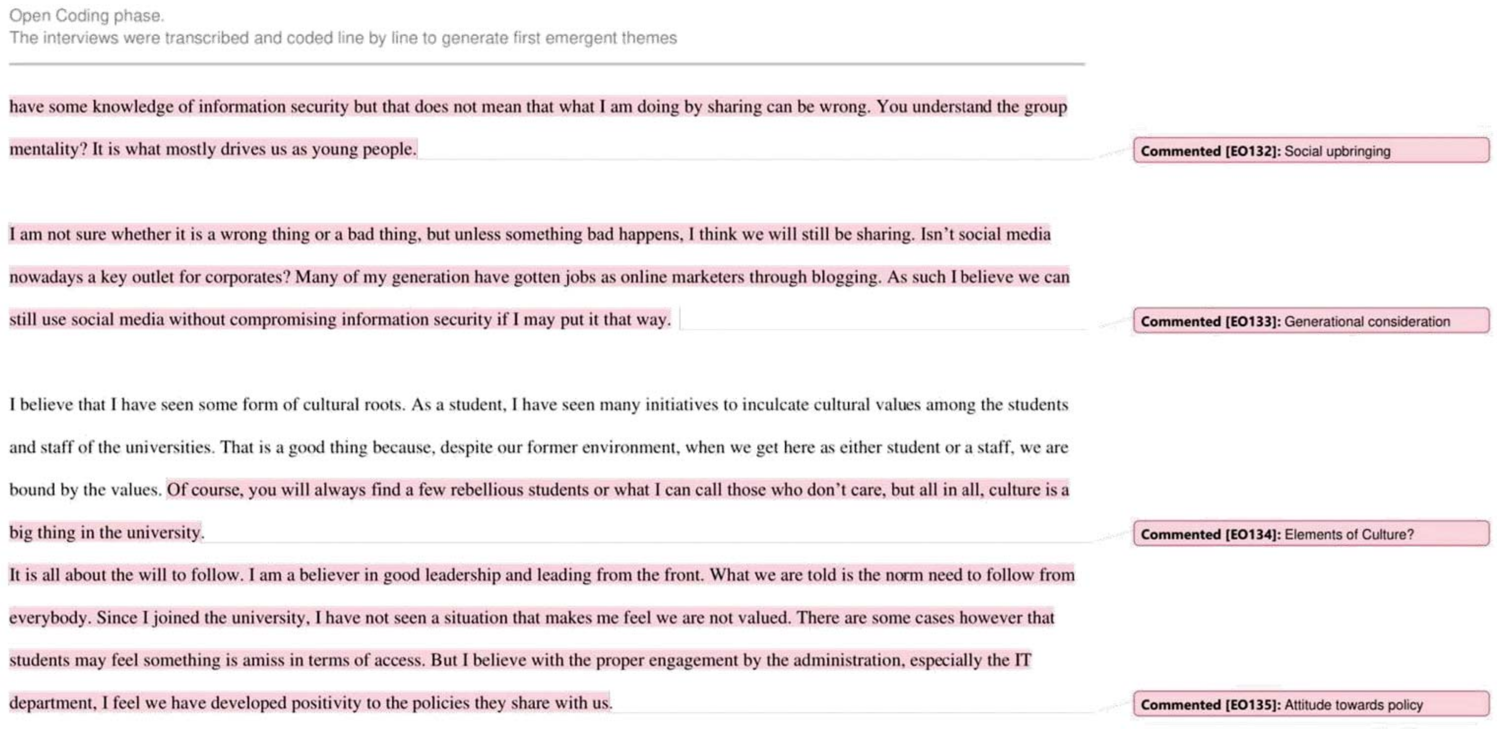
Commented [EO130]: Education background is a factor

I also feel that to some extent, how people are socially natured reflect on how they interact with rules and regulations. This is my opinion though. So, to some extent, I believe that it is not all of those who are in the computer science are likely to go against the rules and violate policies, some of these students are law abiding and we have very few cases of those who socially brought to believe that they have the rights and freedoms to explore. We are however aware of these kinds of students and have provisioned for managing such. It is challenging, but achievable.

Commented [EO131]: Social upbringing

Informant 9: Student – University A

We are a group of students who are in the habit of sharing everything and anything online from our selfies to the most hilarious events that we come across. It is a team thing and we don't feel anything about it. Social media is our lives. And that is why we have never considered it a threat to data security. Of course, there are policy of non-disclosures but whoever reads them and who ever follows them? My opinion is that even if there are rules of what to share and what not to share, there needs to be a way of just filtering them rather than blocking people like us. I



Open Coding phase.
The interviews were transcribed and coded line by line to generate first emergent themes

have some knowledge of information security but that does not mean that what I am doing by sharing can be wrong. You understand the group mentality? It is what mostly drives us as young people.

Commented [EO132]: Social upbringing

I am not sure whether it is a wrong thing or a bad thing, but unless something bad happens, I think we will still be sharing. Isn't social media nowadays a key outlet for corporates? Many of my generation have gotten jobs as online marketers through blogging. As such I believe we can still use social media without compromising information security if I may put it that way.

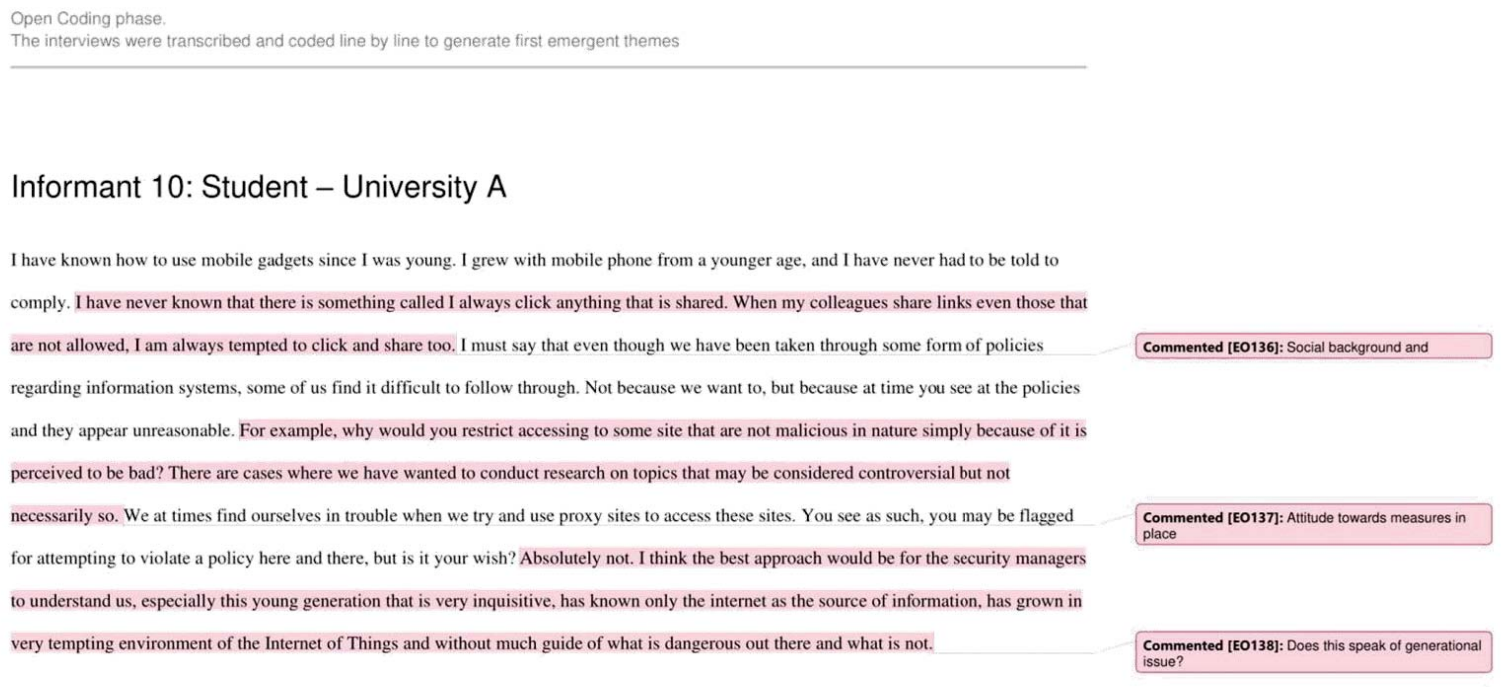
Commented [EO133]: Generational consideration

I believe that I have seen some form of cultural roots. As a student, I have seen many initiatives to inculcate cultural values among the students and staff of the universities. That is a good thing because, despite our former environment, when we get here as either student or a staff, we are bound by the values. Of course, you will always find a few rebellious students or what I can call those who don't care, but all in all, culture is a big thing in the university.

Commented [EO134]: Elements of Culture?

It is all about the will to follow. I am a believer in good leadership and leading from the front. What we are told is the norm need to follow from everybody. Since I joined the university, I have not seen a situation that makes me feel we are not valued. There are some cases however that students may feel something is amiss in terms of access. But I believe with the proper engagement by the administration, especially the IT department, I feel we have developed positivity to the policies they share with us.

Commented [EO135]: Attitude towards policy



Open Coding phase.
The interviews were transcribed and coded line by line to generate first emergent themes

Informant 10: Student – University A

I have known how to use mobile gadgets since I was young. I grew with mobile phone from a younger age, and I have never had to be told to comply. I have never known that there is something called I always click anything that is shared. When my colleagues share links even those that are not allowed, I am always tempted to click and share too. I must say that even though we have been taken through some form of policies regarding information systems, some of us find it difficult to follow through. Not because we want to, but because at time you see at the policies and they appear unreasonable. For example, why would you restrict accessing to some site that are not malicious in nature simply because of it is perceived to be bad? There are cases where we have wanted to conduct research on topics that may be considered controversial but not necessarily so. We at times find ourselves in trouble when we try and use proxy sites to access these sites. You see as such, you may be flagged for attempting to violate a policy here and there, but is it your wish? Absolutely not. I think the best approach would be for the security managers to understand us, especially this young generation that is very inquisitive, has known only the internet as the source of information, has grown in very tempting environment of the Internet of Things and without much guide of what is dangerous out there and what is not.

Commented [EO136]: Social background and

Commented [EO137]: Attitude towards measures in place

Commented [EO138]: Does this speak of generational issue?

Open Coding phase.
The interviews were transcribed and coded line by line to generate first emergent themes

Informant 11: ICT Student – University B

I am from a computer science background as my studies. So, your question on whether this has impacted on how I perceive information security elated issues, well, I can say that I understand the risks that usage of information security or cybersecurity poses when we interact with ICT, however, for me, and I believe most of us as student, what matters is whether the policies work for us in terms of helping us do our studies and learn, or against the interest of us achieving it. What do I mean by this? Simple, if the policies are too restrictive that does not allow anyone to do their studies in a flexible way, many will try to circumvent it. And I have seen many students, especially in the computer science department who try to use tricks known to them to get that pirated software for their programming needs. Same goes to the ease of comprehending what the policies mean. If it is as simple as ABCd, then many will follow the policies. But if the policies themselves are not self-explanatory, then the rationale is lost, and what would be left would be a case of those who want to follow and apply the policy being forced to circumvent it. I have seen very little of the incidents where major policies have been breached by the students that I am close to, but that does not mean it is not happening. These are just my thoughts. I am more likely to comply if I believe that the policies will not harm me in any way. It is virtually every human instinct. But to say the least, I have not had such options. Here in the university we are treated well and given all avenues to express our difficulties. I have not felt that my personal rights are infringed like privacy. But should I feel so, I will avoid complying if I can.

Commented [EO139]: Education background can either have a good result or a bad result

Commented [EO140]: Ease of applying the policies

Commented [EO141]: Perceived risk of applying ISP

Informant 12: Non-ICT student - University B

I believe that social background has a lot to contribute to how policies are complied with. I came from not a well-off family, and I have tried to be as conservative as I possibly can, though in contrast, I see many of my student colleagues who came from wealthy background and who had everything in their way. I see them every day. Though this is not the case with all the students. But if you ask me, there are those who will just go against the grains. What am happy about is the fact that the university authority has been very impactful in creating awareness on the risks. This has made even those who would be violating the policies unconsciously to be on the right side. And even though I may not be able to fully confirm this, I believe that there is a positive culture of information security policy compliance. It is very difficult to follow a rule if you know it will get back to you. Rules, or policies for that matter, should never be used as a tool to harm someone. That, however, is different when I am told in advance that this is what we are collecting, this is what we are using to track, and this is the reason. Do this and Do not do this, and this are the reasons. I that is made clear, I do not think any reasonable person can be mad about it. Policies are there and I, for instance, know that when I log in to the university WiFi, I am openly being monitored. So, it can also act as a deterrence

Commented [EO142]: Aspects of social upbringing

Commented [EO143]: Signs of awareness creation by the institution

Commented [EO144]: Positive indication of culture of compliance

Commented [EO145]: Perceived risks of ISP application

Informant 13: Non-ICT Staff – University A

I am aware of several polices in place already, though what I am not sure is how that have worked towards addressing information security policies. I am a staff in a non-Information Technology area of profession. But despite that fact, we have been constantly trained on how to understand the policies. I am glad of the fact that the institution is keen on having a population that understands and is constantly aware of the threats posed by usage of the information systems.

Commented [EO146]: Awareness towards the policies

In terms of dealing with compliance or non-compliance, I believe there is a system to handle such. What I have seen in the past is a process of informing the would-be violators about the possible policy violations especially when trying to access restricted resources. I have always seen screen prompts in my computer when I accidentally bump on a website that is restricted. But I believe this does not constitute a violation. However, like in any given society, there may be those who may deliberately attempt to bypass these policies and I believe there is a way that the institution will handle them. By and large, I have not heard any of my colleagues being confronted with accusations of policy infringement that warrants serious punishment.

Commented [EO147]: Belief in the system, controls in place

Speaking from my own experience, I have been in the institution for more than 10 years working in different section, my experience has drawn me to the view that we have a strong culture of complying with policies. I see my superiors are also very keen on following guidelines which if you ask me, is a positive gesture from top management. I believe that this is one thing that also encourages others in the lower sections be it staff or students to also comply with whichever policies that are in place. We have a strong culture in the university, and this is beyond just the information security policies. We are a certified institution through the ISO certification and as such, I believe that part of the reasons to qualify is the aspect of strong culture of compliance with international standards which are contributed largely by the staff and students. So, culture, if you ask me, is much stronger in terms of individual and institutional compliance.

Commented [EO148]: Strong compliance culture

Commented [EO149]: Management leading by example

Informant 14: Non-ICT Student – University B

To some extent, students like us are difficult to deal with. If even among ourselves we find it a challenge to work and follow our own rules, I can imagine what the management must contend with. I mean, we have some students who are naturally rebellious. Even when we are in our own groupings like class group, you will find a few who do not follow what we have all agreed on. And this is hurting and disappointing. When the same students violate information security, they feel good about it. My worry is that this also makes others follow them blindly. Is it a good thing? I do not think so. You asked about what I can say about the culture in the university. To answer that, I would say that yes, I believe we

Commented [EO150]: Rebellious attitude towards policy have a culture as a university. The culture, especially around the information system related culture can be seen in how the management and the student handle issues related to policies. Our university, and by that I would like to restrict myself to the campus, has done a great job in creating awareness. We have accessible ICT office in case one feels the need to make a query. We have access to the student portal. The portal is well secured and is always available. We have WIFI everywhere and though I am not from IT background, I feel secure when I browse using the WiFi hotspots. But all in all, I have also seen many communication updates on potential risks that we may be exposed to if we are not careful.

Commented [EO151]: Culture?

Commented [EO152]: Awareness programs

Informant 15: Non-ICT Student – University A

I believe there is information security culture. We do get occasionally alerts of potential risks in our emails from ICT office. This helps us prepare. In fact, when I came in as a student 3 years ago, I was bombarded with a lot of information about information systems policy. And I think this is a good this. You know, if the students and staff have such kind of information, then one has no reason to go against it.

Commented [EO153]: Information security policy compliance culture

But of course, we have those who cannot just do the right thing. By this I mean the bad apples in the family. I have seen a lot of students like me who are conscious about their privacy and do all they can to ensure they are secure from online risks, but then there are those who are just wired. What they do not know is that they expose their own private information and pose a risk to the university systems.

I may not be from an ICT related background, but as one who has grown in the [dotcom] era, I believe I have the basic understanding of cybersecurity issues. But so far, I have not seen any student going as far as hacking. But who knows what happens in the dark? What I have seen is more of the group dynamics. It is evident when you interact with some of my student colleagues. When one can access the allowed sites, everyone will want to do so and even more than just accessing the sites.

Informant 16: Staff (Non-IT) University A

To answer your question, I believe we have an established culture in the university that enables us to comply with policies. I know of efforts that have been made for new and old members to feel that they are part of the university community. When you walk into the university, you will notice that the way staff and student alike carry themselves speaks of a culture that speaks of respect to the norms and values. For example, did you notice how students and staff obey simple regulations such as presenting their identifications when accessing the buildings? That is what I call simple culture of compliance. And I have seen the same with the area of information technology. The university management has entrusted us to be the role model to the younger members such as the students. We have been involved in many trainings to ensure we are aware of cyber risks even as we perform our duties. Well, I have not heard of major breaches, maybe it is because I am not in the ICT department. But in most cases, the ICT department usually informs if there are development. As a staff, I believe there are standards that the university has to meet especially in the delivery of its mandate. These are usually informed by external regulations and of course what others have done best. So, what I

Commented [EO154]: Semblance of compliance culture would say is that we also borrow a lot from what other organizations have done to inform how we strategies. This is not only in the area of ICT related policies but also in the way we do business. I am from the library management background. So, standards and regulations are our day to day food to nature how we do business. When it comes to the culture of integrating behavior in our clients who are both students and staff, what I would say is that at times dealing with the younger generation is hectic as compared with dealing with older mature generation. When I talk about maturity here, I do not mean age, but the reasoning capacity. [**Can you clarify**] I have seen many younger generations who reason in the best interest of everyone especially when they are told what not to do and how not to do things. For example, when we talk about library access and how to behave in the library, there are rules, at times the younger generation conduct themselves in a mature manner better than the older generation who may want to show how senior they are. So, to me maturity here is not about age, but about reasoning capacity.

Commented [EO155]: Maturity of individuals

Commented [EO156]: A new angle about maturity.

Informant 17: Technical Staff – University B

We deal a lot with issues compliance because we have to make sure everyone does so. My day to day responsibilities are to monitor the usage of the network and other ICT infrastructure. My experience with the students who are from the IT background is very challenging. Many have attempted to go against the rules of accessing pirated software within the network. But thanks to our strong firewalls, no one has so far managed to get through. But what does this tell you? It shows that as opposed to non-IT students, the non-IT related students rarely get to attempt breaching the rules of what to access. We know this because each student and staff have access based on their student ID and we can monitor the traffic to know who is accessing what. That is why everyone is told to be responsible for the usage of their login ID. What we have done so well and successfully is to create awareness. However, to efforts that we make are deeply dependent also on how management supports us. This has been the best ingredient for our successful information security culture. With the support, we have made sure that stronger and robust contributions are made towards awareness creation and campaigns. We have seen several responses from the students and faculty as well as non-teaching staff who use the university's ICT assets who have asked queries. This shows us that everyone is interested to be part of the culture. Some of our rules are drawn from a diverse source such as the national and international regulations. We have standards that contributes to how we do things. A case example is the NIST standards that we have been studying to see how we can embed in our cybersecurity frameworks.

Here at home we also have governing bodies such as Communications Authority who monitors how we run information systems assets. We are also guided by the International Certification standards. We have just to maintain this and strive to be on top. In addition, we also believe as an institution that learning from best practice help strengthen our initiatives. Why would we reinvent the wheel when it works somewhere already? We can improve on what works and redevelop what does not work. With regards to culture, we have a strong culture not only in information security area, but in general, we are a compliant society. I have seen this after many years in this institution.

Commented [EO157]: Information Security culture with support of the management

Commented [EO158]: Best Practices from peer

Informant 18: Non-Technical Staff – University A

I have no idea about information security related issues. But a have a rough idea about what you are talking about. Maybe I can talk about my background as staff in the administration person. I deal a lot with face to face queries from students and staff a lot. What I can say is that we have a culture of respect for diversity. But I will tell you that students are from different backgrounds. There are those who are just too difficult to handle while others are easy because they understand when one explains something. This is my opinion though, whenever I probe further those who are difficult, you come to realize one common thing about them. They will mostly be coming from a social background of being spoilt. So, I always wonder silently, why one would behave the way they do. But anyway, that is them. Back to the issues, students and staff are from various backgrounds and there are those who have been brought up in a respectful way and there are those who have been brought in what I want to call a self-entitlement way. By this I mean, there are those who will irritate you because they feel entitled. But I am happy to say that despite this, our training is such that we have to find a way of managing all these backgrounds. In terms of security, as I had said, I have no idea what cybersecurity is, but I have always seen emails alerting us about being careful with clicking links anyhow in our inbox. I guess those in charge of our internet are aware of these possibilities. So, I would say there is some form of monitoring. This is a good thing since it shows a system that works in that front. We are a mature culture, and management is always at the front leading by example. This one I can attest to myself as a staff with many years in this university.

Informant 19: Student University B

Asked about the peer mentality and how it would affect information security policy compliance, "Most of my colleagues will agree with me that what drives us is the group mentality. I know this might sound funny. But I am also at time driven by that. I find it mind boggling to belong even if it may have negative effect. We go drinking, we go clubbing, and then when we are back in our hostel, we go online in the internet to watch movies. This we do in total disregard to the restrictions that we have. There have been issues raised with internet blockages. But we always find a way around. What do they expect we do? Honestly? I have friends who understand these things. I mean those who are doing computer science. They help us a lot those who are not conversant with these things. We get also videos from them. You know the thing about torrents? I know many will say the internet is blocked. But they know how to override the blockade. I think they use firewall blocker or something like that. Anyway, I do not have much to say about it". ***Regarding question about culture, the student had this to say***, "I believe there is a culture of compliance, but as you have already heard, some restrictions are just too much and we have to find a way out. It is not right, but what do we do? I believe if no one understands the reasons behind what the admin does or why we do some things, there will always be violators". ***How about your thoughts on the role played by generational aspect on compliance with policies?*** "I am student who is used to social media sharing, and as such, I find it difficult to resist sharing any information that I find interesting to share"

Commented [EO159]: Peer pressure

Commented [EO160]: Acknowledgement of compliance culture

Informant 20: Student University B

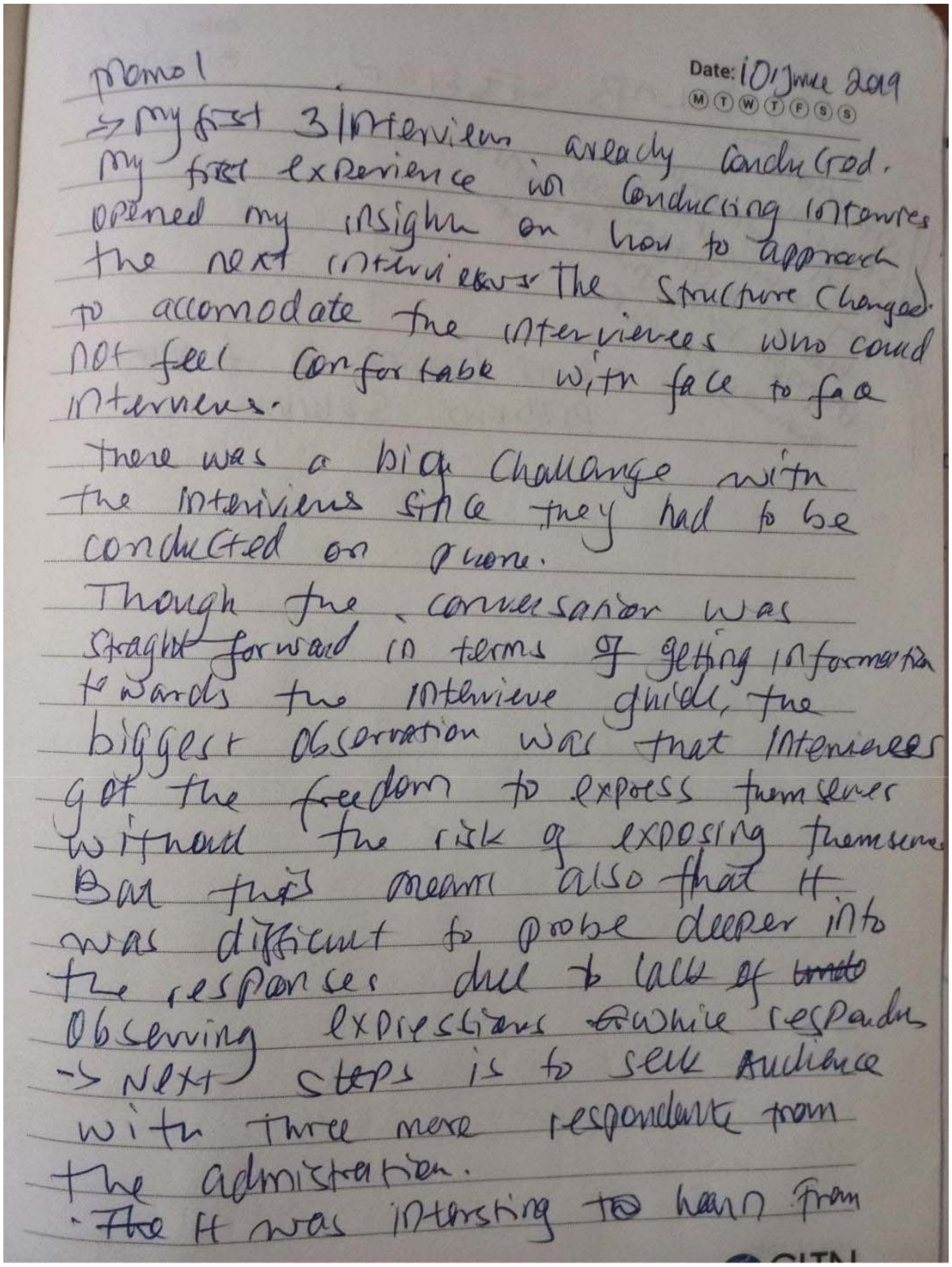
When asked about what the student thought about maturity level with regards to compliant behavior, the student had this to say. "I have seen a lot of mt colleagues complaining a lot about the rules that they have to follow especially since they are restricted to access some site. A lot is dependent on how mature one is. Most of those I have seen complaining are the new students who have not stayed long here. They are still getting to learn that this is not a place to access everything one wants to what." ***Why do you say so?*** "you know, when we were in high school, we rioted for just being told we cannot watch TV in certain days. This is not high school. But then again, I at times understand the comrades. Sometimes you just want space to relax and watch movies. We believe in torrents which have been blocked, you know? But what I usually do is not to through tantrums and start breaking the rules, but I buy my own bundles". "I blame these temptations of violations on the perceptions that we have as student. You know when one refuses you to do something without knowing why?"

As a student, what can you say about the administration's information security policy compliance actions? "what I can say is that we do get reminders in our emails and occasionally, we would have warnings in our screens when we attempt to violate the policies. So, with regards to information security policies in place, we are aware. It is only that there is a difference between being told to do something, and the attitude that once has towards some rules." ***So, what do you mean about attitudes?*** "what I mean is that the attitude one has toward policies would determine if these policies are adhered to. That's all." ***What about information security culture? What would you say about culture in this university?*** "all I can say is that I believe we have an embedded culture as a university. This, I can say is drawn from the history that this university has since I started knowing it while I was young. However, with regards to information security culture, I am not sure whether to say there is a strong culture or not. I can only speculate that there is one because of not so many reports on compromises. Culture or no culture, I grew with mobile

Commented [EO161]: Some feeling of cultural presence phone from a younger age, and I have never had to be told to comply. I always click anything that is shared. I believe this to be the case with many of my peers."

Commented [EO162]: Social Upbringing

APPENDIX 11: Constant Memoing Excerpts



memo1

Date: 10 June 2019
M T W T F S S

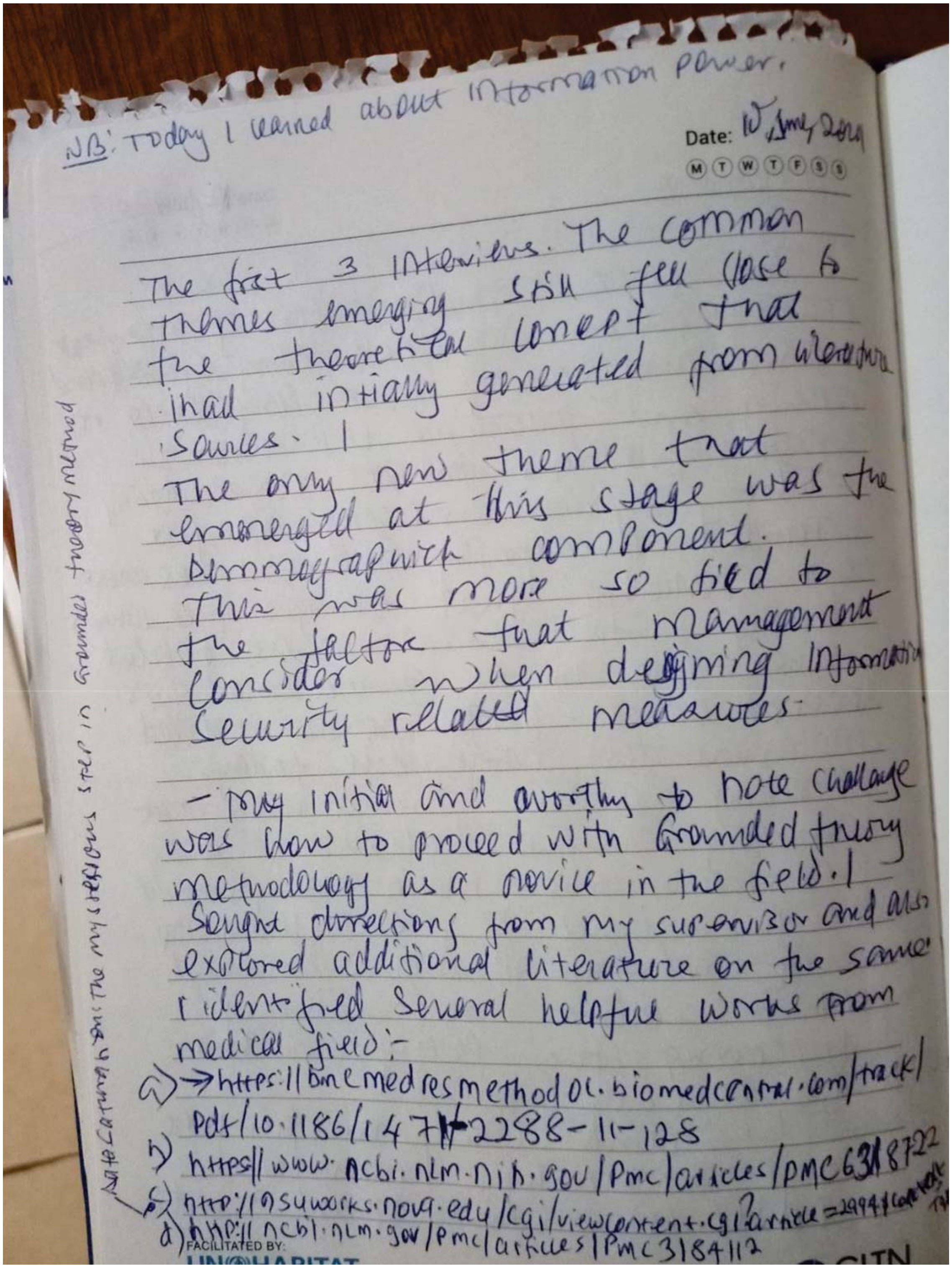
-> my first 3 interviews already conducted. My first experience in conducting interviews opened my insight on how to approach the next interviewers. The structure changed to accomodate the interviewees who could not feel comfortable with face to face interviews.

There was a big challange with the interviews since they had to be conducted on phone.

Though the conversation was straight forward in terms of getting information towards the interview guide, the biggest observation was that interviewees got the freedom to express themselves without the risk of exposing themselves. But this meant also that it was difficult to probe deeper into the responses due to lack of ~~[illegible]~~ observing expressions while respondin

-> Next steps is to seek audience with three more respondents from the administration.

· ~~The~~ It was intersting to hear from



NB: Today I learned about Information Power.

Date: 10, June, 2019

Ⓜ Ⓣ Ⓦ Ⓣ Ⓕ Ⓢ Ⓢ

The fist 3 interviews. The common themes emerging still fell close to the theoretical concept that i had initially generated from literature sources.

The only new theme that emergeld at this stage was the Demmographic component. This was more so tied to the factor that management consider when designing Information Security related measures.

- my initial and worthy to note challange was how to proceed with Grounded theory methodology as a novice in the field. I sought directions from my supervisor and also explored additional literature on the same. I identified several helpful works from medical field:-

a) → https://bmcmedresmethodol.biomedcentral.com/track/pdf/10.1186/1471-2288-11-128

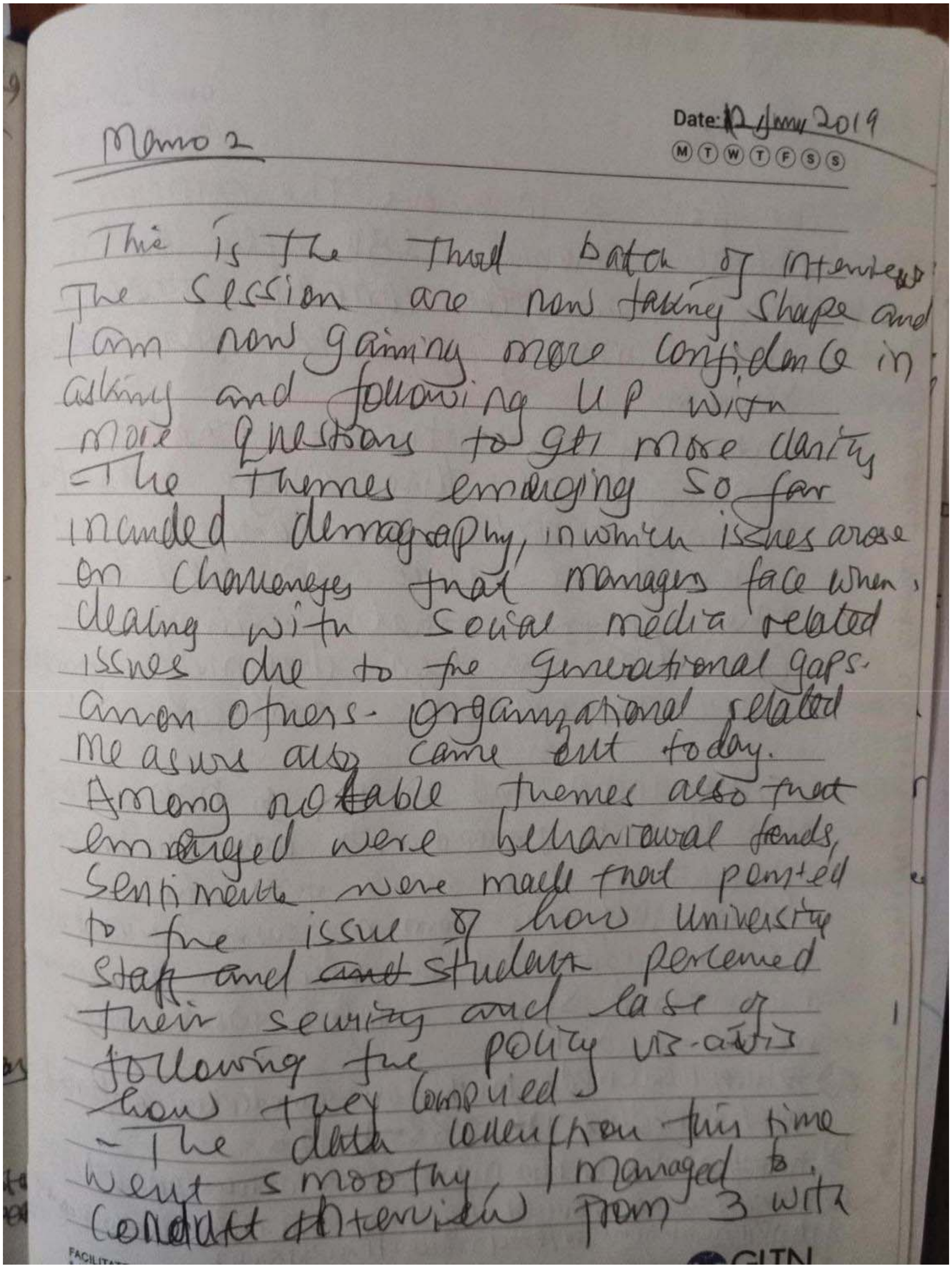
b) https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6318722

c) http://nsuworks.nova.edu/cgi/viewcontent.cgi?article=2994&context

d) http://ncbi.nlm.gov/pmc/articles/PMC3184112

Data Categorization: The mysterious step in Grounded theory method

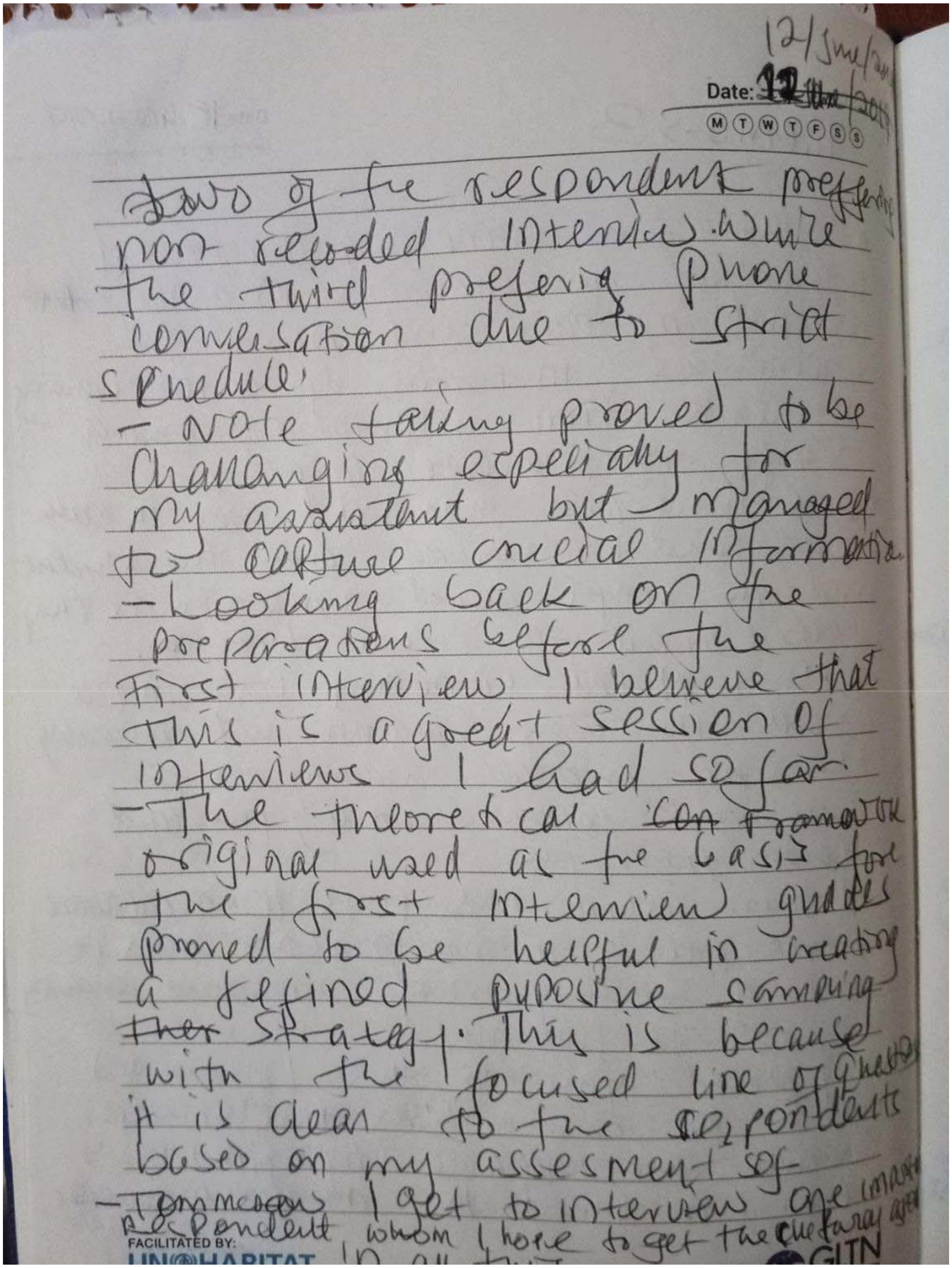
FACILITATED BY:



Memo 2

Date: 12 June 2019
M T W T F S S

This is The Third batch of interviews
The session are now taking shape and
I am now gaining more confidence in
asking and following up with
more questions to get more clarity
- The Themes emerging so far
included demography, in which issues arose
on challenges that managers face when
dealing with social media related
issues due to the generational gaps
among others. Organizational related
measure also came out today.
Among notable themes also that
emerged were behavioural trends,
sentiments were made that pointed
to the issue of how University
staff and ~~and~~ students perceived
their security and ease of
following the policy vis-a-vis
how they complied.
- The data collection this time
went smoothy, I managed to
conduct interview from 3 with



12/June/2019

Date: ~~12 the~~/2019

M T W T F S S

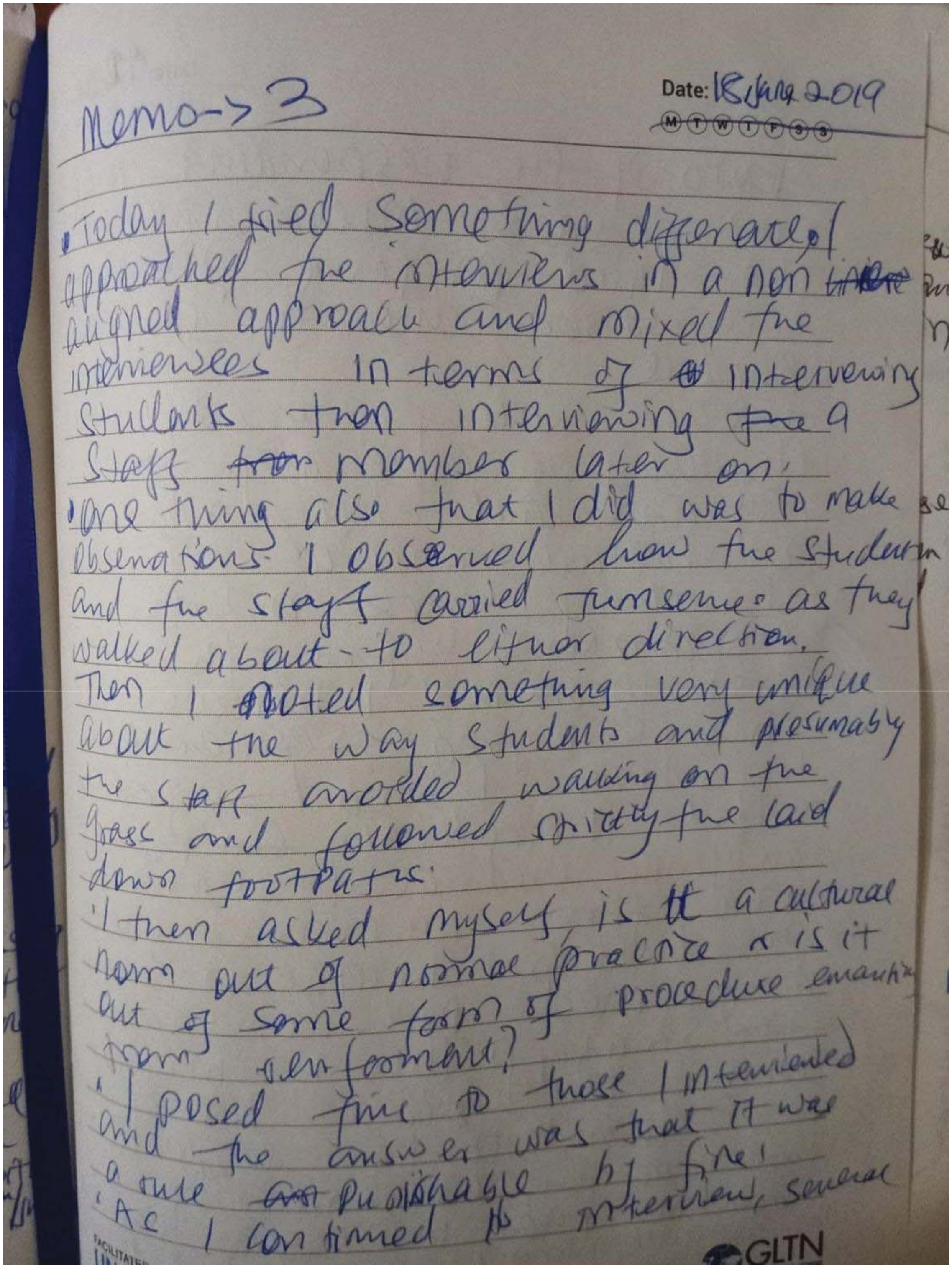
two of the respondent preffering non recorded interview. While the third prefering phone conversation due to strict schedule.

- Note taking proved to be challenging especially for my assistant but managed to capture crucial information
- Looking back on the preparations before the first interview I believe that this is a great session of interviews I had so far.
- The theoretical ~~con~~ framework original used as the basis for the first interview guides proved to be helpful in creating a defined puposive sampling ~~ther~~ strategy. This is because with the focused line of questions it is clear to the respondents based on my assesment sof
- Tommorow I get to interview one important respondent whom I hope to get the clarifying [illegible] in all

FACILITATED BY:

UN-HABITAT

GLTN



Memo -> 3

Date: 18 June 2019

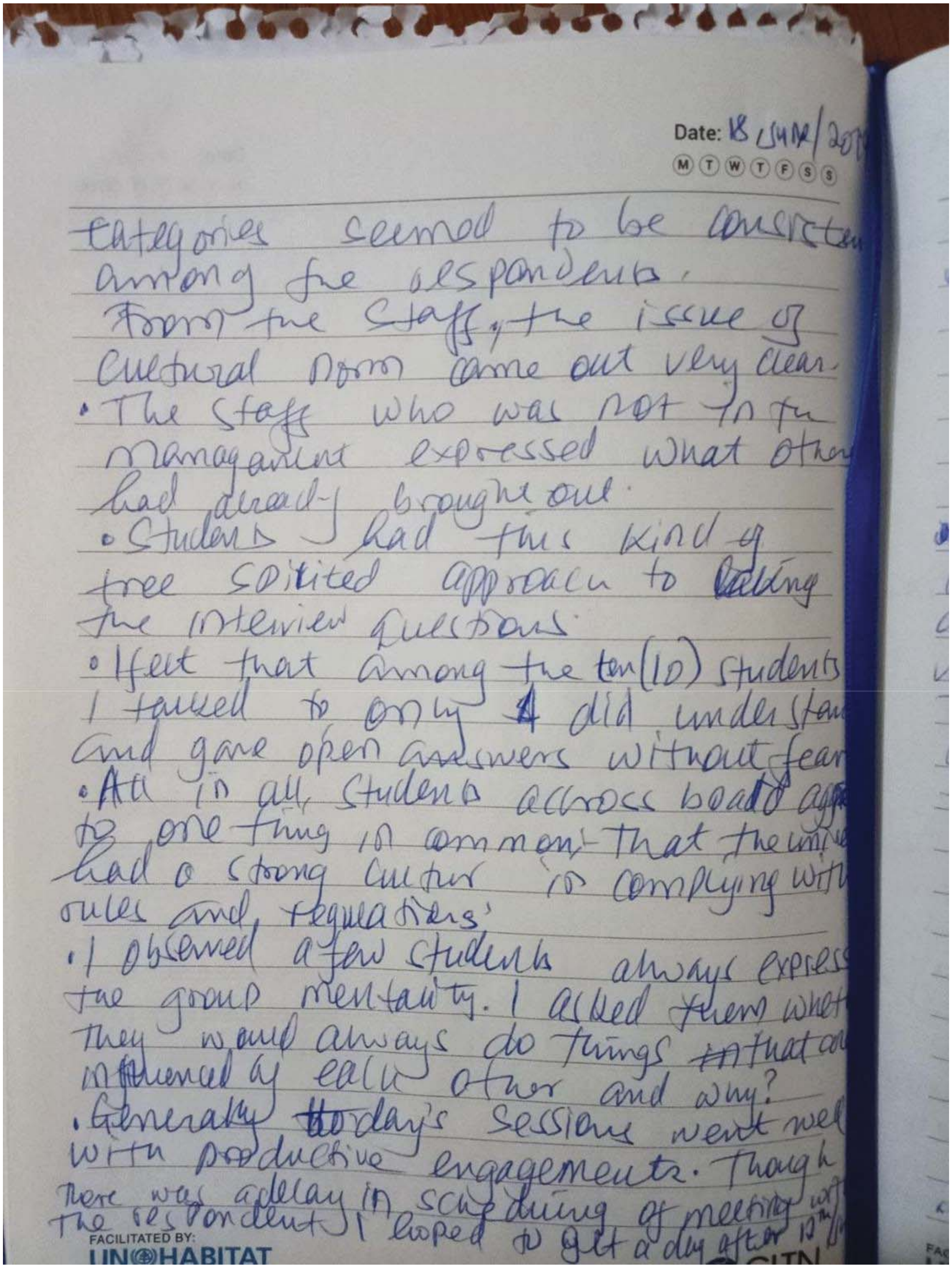
M T W T F S S

- Today I tried something differnatly. I approached the interviews in a non ~~[illegible]~~ aligned approach and mixed the interviewees in terms of ~~a~~ interviewing students then interviewing ~~the~~ a staff ~~from~~ member later on.
- One thing also that I did was to make observations. I observed how the students and the staff carried themselves as they walked about - to either direction.

Then I noted something very unique about the way students and presumably the staff avoided walking on the grass and followed strictly the laid down footpaths.

- I then asked myself, is it a cultural norm out of normal practice or is it out of some form of procedure emanating ~~from~~ enforcement?
- I posed this to those I interviewed and the answer was that it was a rule ~~an~~ punishable by fine.
- As I continued to interview, several

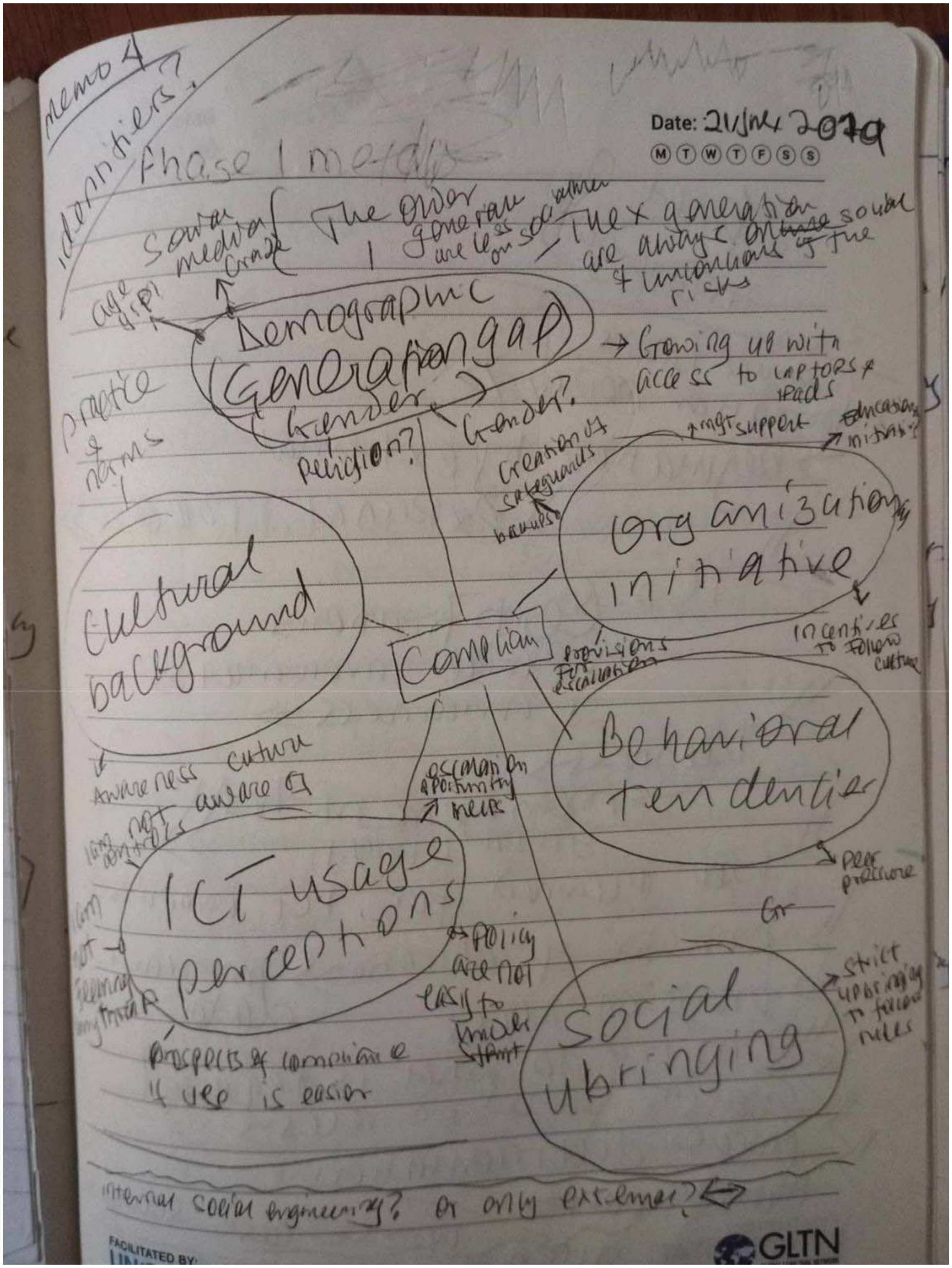
GLTN

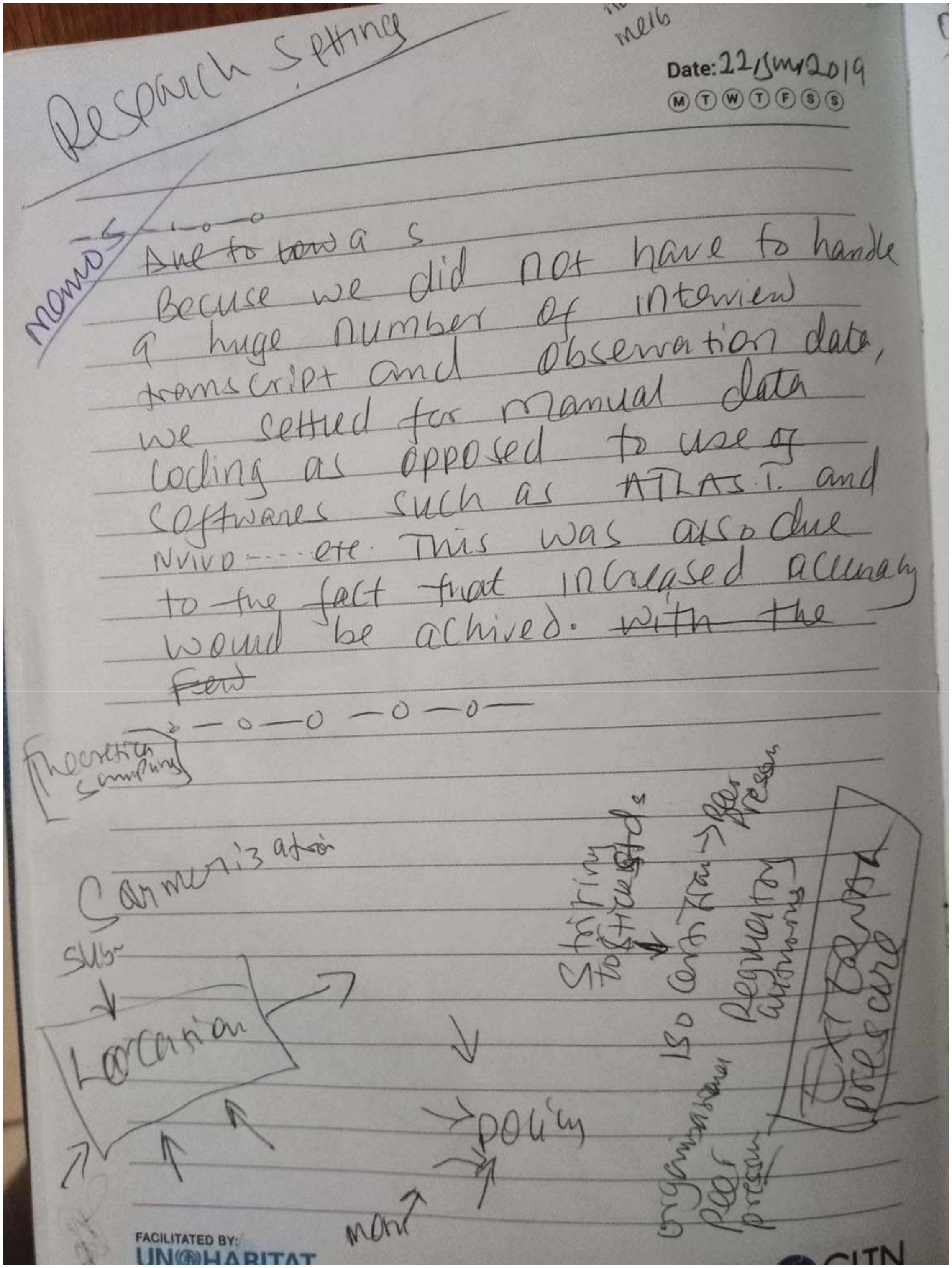


Date: 18 JUNE/201
M T W T F S S

categories seemed to be consisten
among the respondents.
From the staff, the issue of
cultural norm came out very clear.
• The staff who was not in the
management expressed what other
had already brought out.
• Students had this kind of
free spirited approach to tackling
the interview questions.
• I felt that among the ten (10) students
I talked to only 4 did understan
and gave open answers without fear
• All in all, students across board agr
to one thing in common: That the unive
had a strong culture in complying with
rules and regulations.
• I observed a few students always express
the group mentality. I asked them whet
they would always do things ~~in~~ that ar
influenced by each other and why?
• Generally ~~to~~day's sessions went wel
with productive engagements. Though
there was a delay in scheduling of meeting wi
the respondent I hoped to get a day after 19th

FACILITATED BY:
UN HABITAT


memo 4
identifiers?
Phase 1 memo
Date: 21/June 2019
Ⓜ Ⓣ Ⓦ Ⓣ Ⓕ Ⓢ Ⓢ
social media
Grade
The older generation are less on social media
The x generation are always on social media & unconscious of the risks
age gap!
Demographic (Generation gap)
Gender
Gender?
Religion?
→ Growing up with access to laptops & ipads
practice & norms
Creation of safeguards
bonuses
mgt support
Educational initiatives?
Organization initiative
incentives to follow culture
Cultural background
Complian
provisions for escalation
Behavioral tendencies
peer pressure
Gr
awareness
culture
aware of
not controls
escalation on opportunity areas
ICT usage perceptions
I am not seeing anything
Policy are not easy to understand
prospects of compliance if use is easier
Social upbringing
strict upbringing to follow rules
internal social engineering? or only external?
FACILITATED BY:
GLTN



Research Setting

mells

Date: 22/Jun/2019

Ⓜ Ⓣ Ⓦ Ⓣ Ⓕ Ⓢ Ⓢ

memos

~~Due to tow~~ a s

Becuse we did not have to handle a huge number of interview transcript and observation data, we settled for manual data coding as opposed to use of softwares such as ATLAS.T. and NVIVO----etc. This was also due to the fact that increased accuracy would be achived. ~~with the Few~~

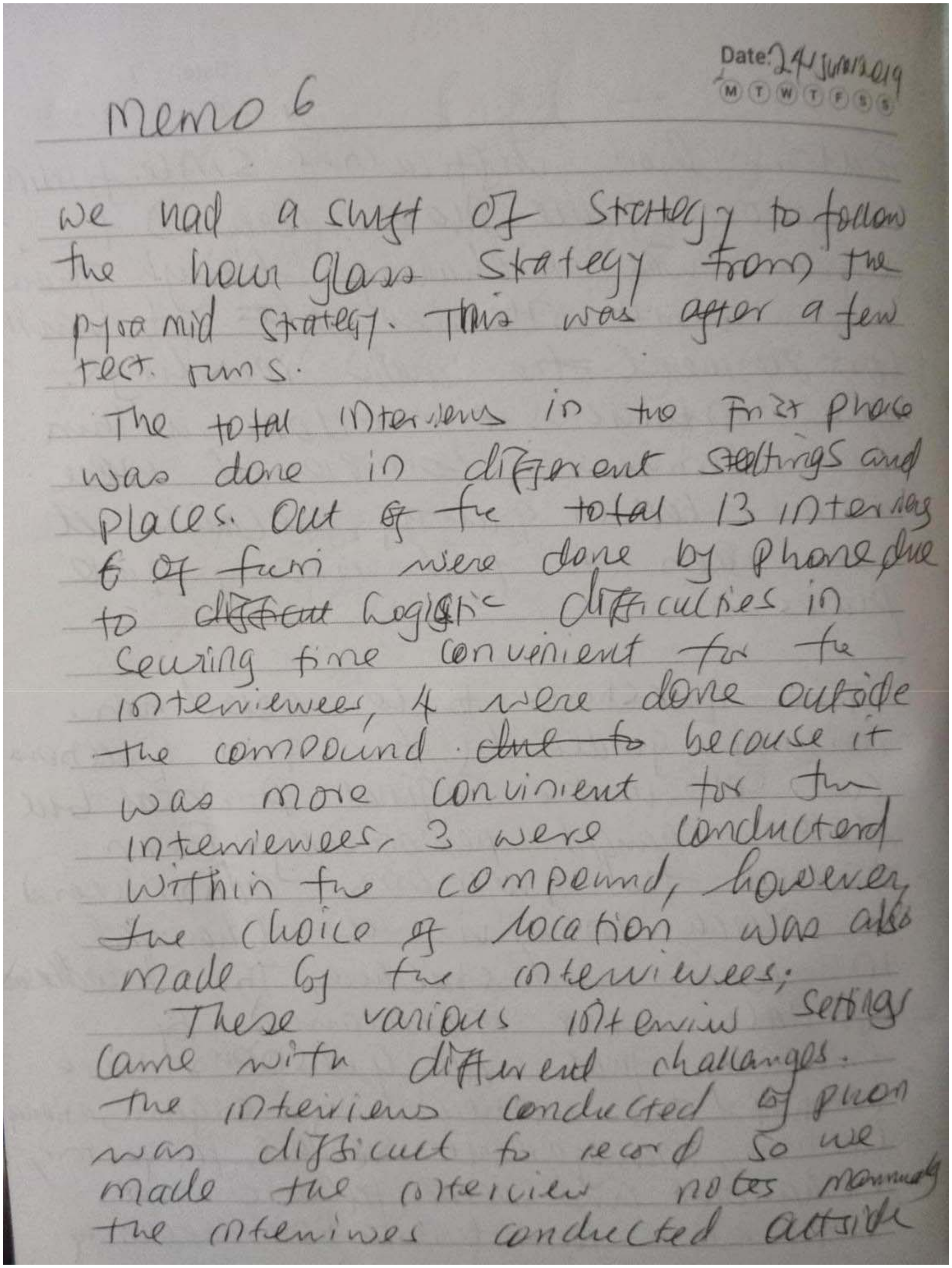
—o—o—o—o—

Theoretical sampling

Commerization
Sub
Location
policy
mon
Striving to Kill stds
ISO certification → peer pressure
Regulatory authority
organizational peer pressure
External pressure

FACILITATED BY:
UN-HABITAT

CITN



Date: 24 June 2019

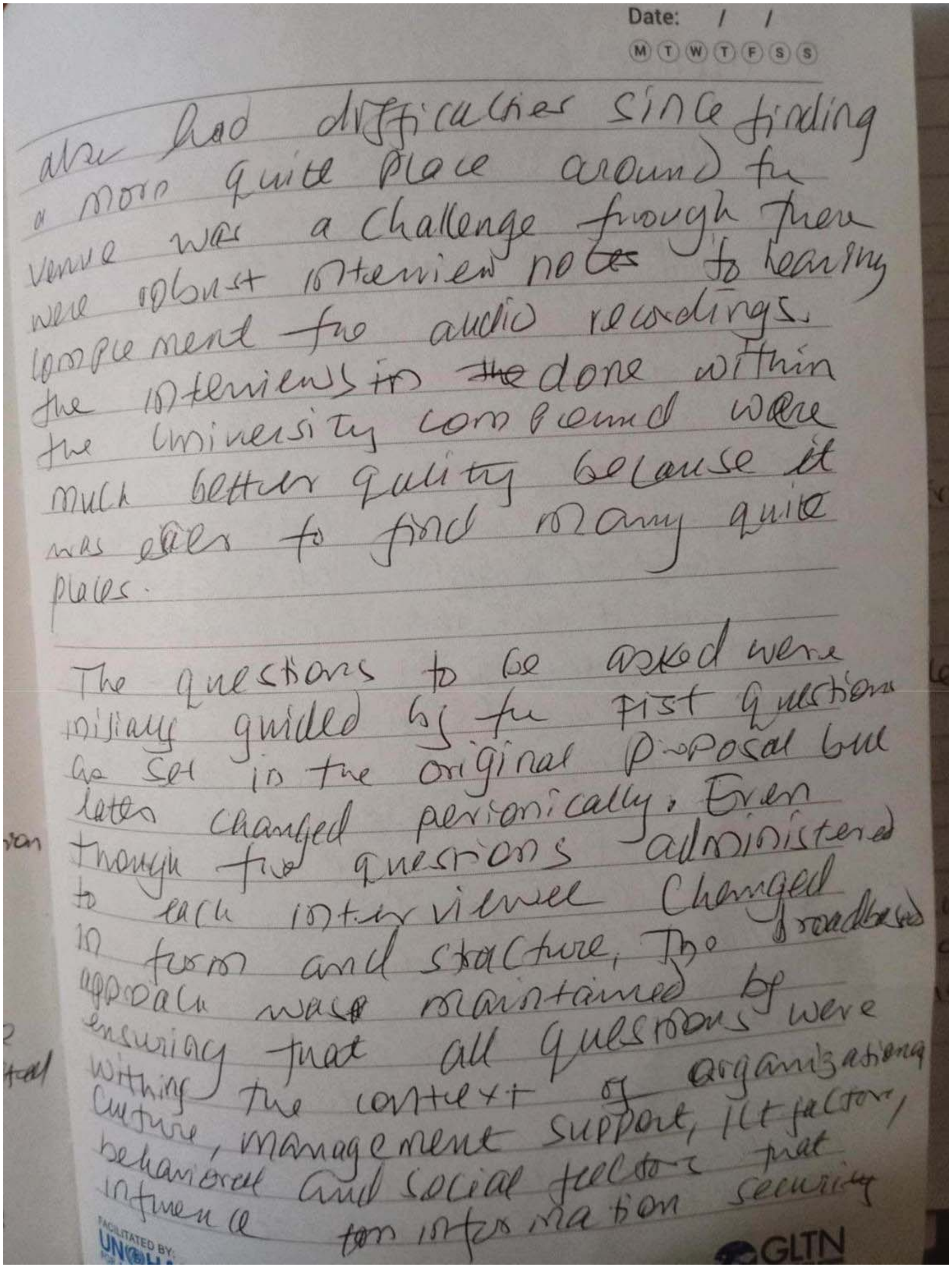
Ⓜ Ⓣ Ⓦ Ⓣ Ⓕ Ⓢ Ⓢ

Memo 6

we had a shift of strategy to follow the hour glass strategy from the pyramid strategy. This was after a few test runs.

The total interviews in the first phase was done in different settings and places. Out of the total 13 interviews 6 of them were done by phone due to ~~difficult~~ logistic difficulties in securing time convenient for the interviewees, 4 were done outside the compound. ~~due to~~ because it was more convinient for the interviewees, 3 were conducted within the compound, however, the choice of location was also made by the interviewees;

These various interview settings came with different challanges. The interviews conducted by phon was difficult to record so we made the interview notes manually the interviews conducted outside



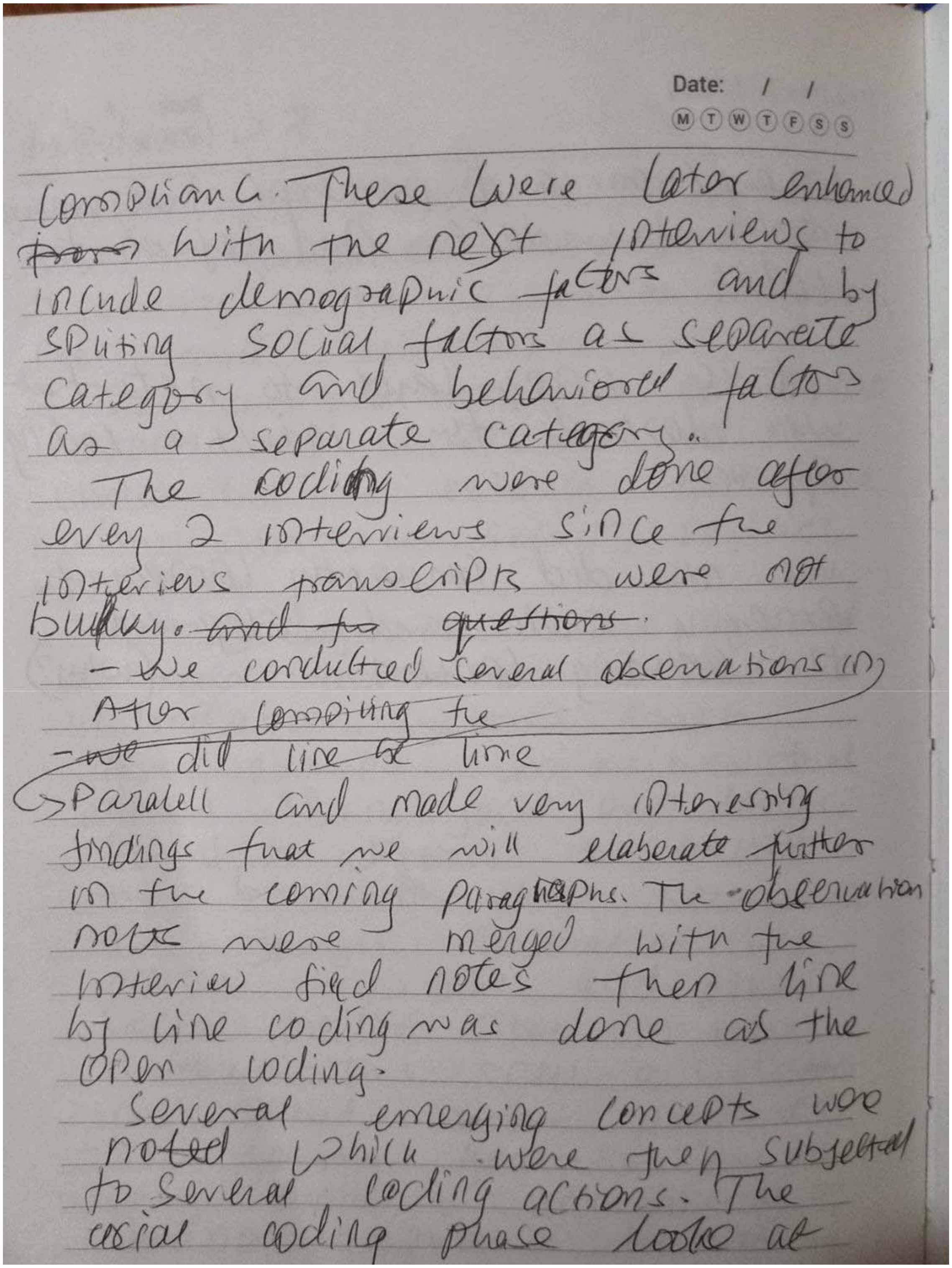
Date: / /

Ⓜ Ⓣ Ⓦ Ⓣ Ⓕ Ⓢ Ⓢ

alsu had difficulties since finding a moro quite place around the venue was a challenge though there were robust interview no~~tes~~ to hearing complement the audio recordings. the interviews in ~~the~~ done within the university compound were much better qulity because it was easer to find many quite places.

The questions to be asked were inisially guided by the fist questions as set in the original proposal but later changed periodically. Even though the questions administered to each interviewee changed in form and structure, The broadbased approach was~~e~~ maintained by ensuring that all questions were withing the context of organizational culture, management support, ICT factors/ behavioral and social factors that influence on information security

FACILITATED BY:



Date: / /

Ⓜ Ⓣ Ⓦ Ⓣ Ⓕ Ⓢ Ⓢ

compliance. These were later enhanced ~~from~~ with the next interviews to include demographic factors and by spliting social factors as separete category and behaviorel factors as a separate category.

The coding were done after every 2 interviews since the interviews transcripts were not bulky. ~~and for questions~~.

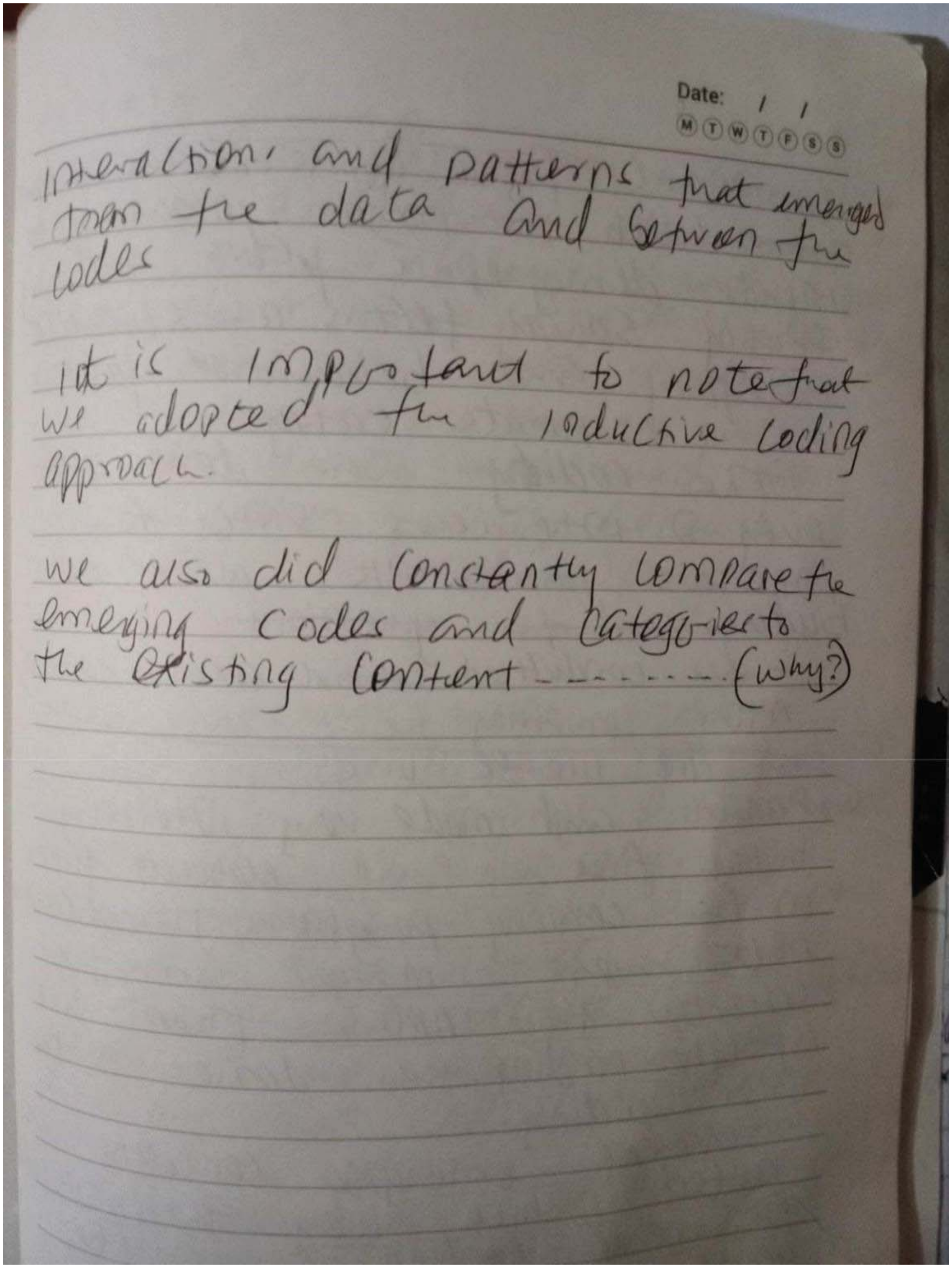
- we conducted several observations in

~~After compiling the~~

~~-we~~ did line ~~by~~ line

Parallell and made very interesting findings that we will elaborate further in the coming paragraphs. The observation notes were merged with the interview field notes then line by line coding was done as the open coding.

Several emerging concepts were noted which were then subjected to several coding actions. The axial coding phase looke at



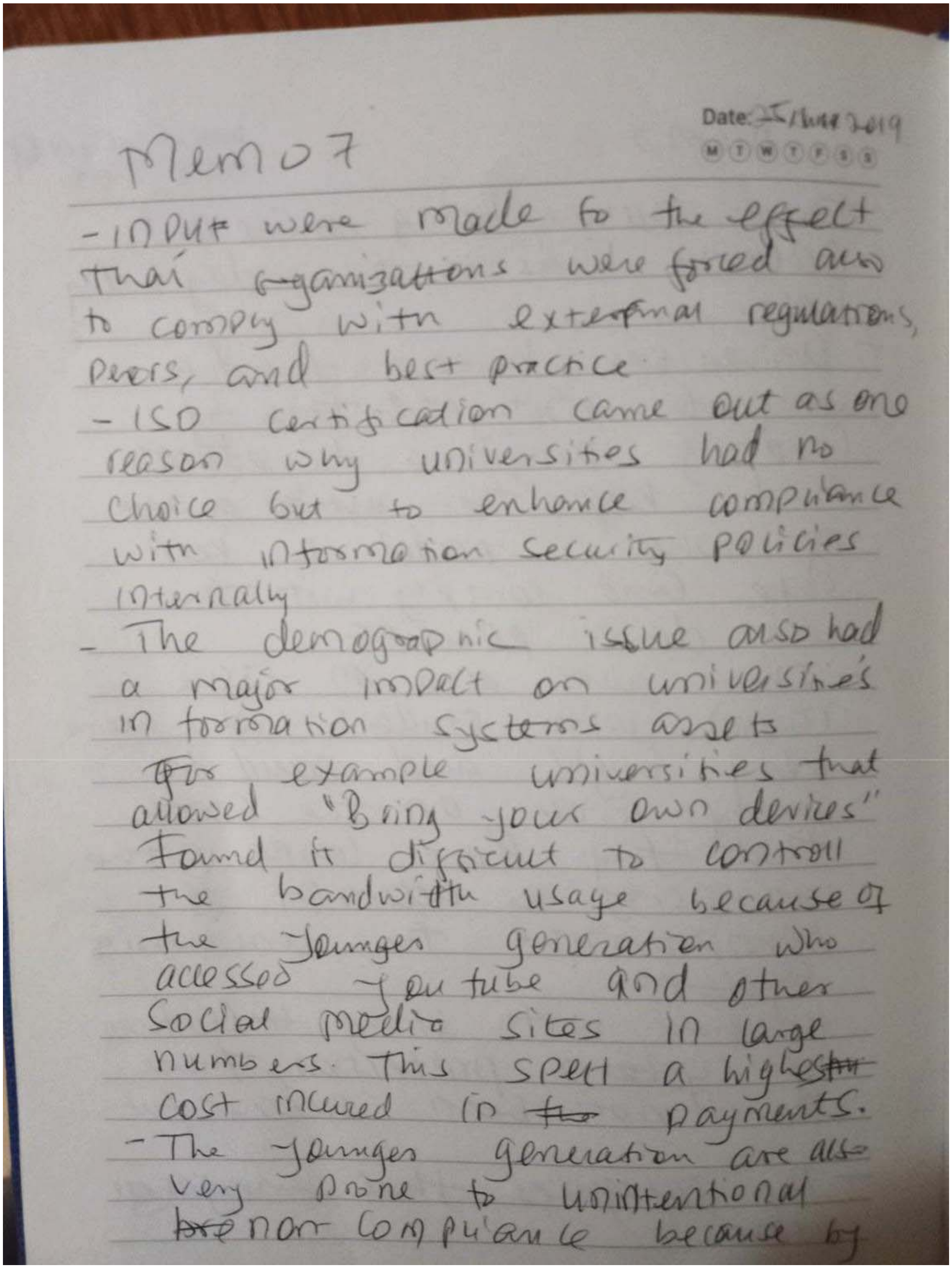
Date: / /

M T W T F S S

interaction, and patterns that emerged from the data and between the codes

it is important to note that we adopted the inductive coding approach.

we also did constantly compare the emerging codes and categories to the existing content -------- (why?)

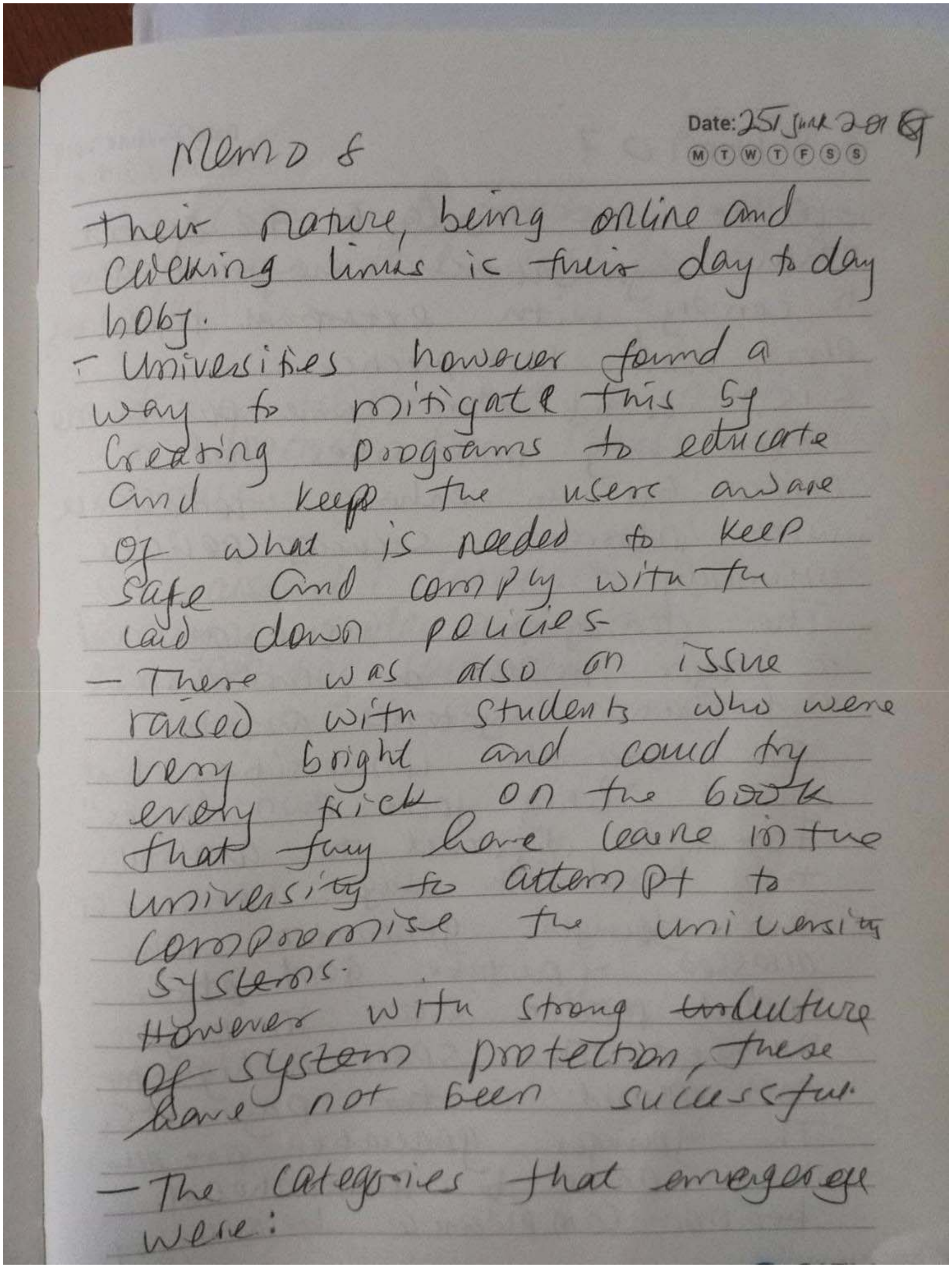


Memo 7

Date: 5 /Mar 2019

M T W T F S S

- Input were made to the effect That organizations were forced also to comply with external regulations, peers, and best practice
- ISO certification came out as one reason why universities had no choice but to enhance compliance with information security policies internally
- The demographic issue also had a major impact on universitie's information systems assets For example universities that allowed "Bring your own devices" Found it difficult to controll the bandwidth usage because of the younger generation who accessed you tube and other social media sites in large numbers. This spelt a highest cost incurred in ~~the~~ payments.
- The younger generation are also very prone to unintentional ~~bre~~ non compliance because by



Memo 8

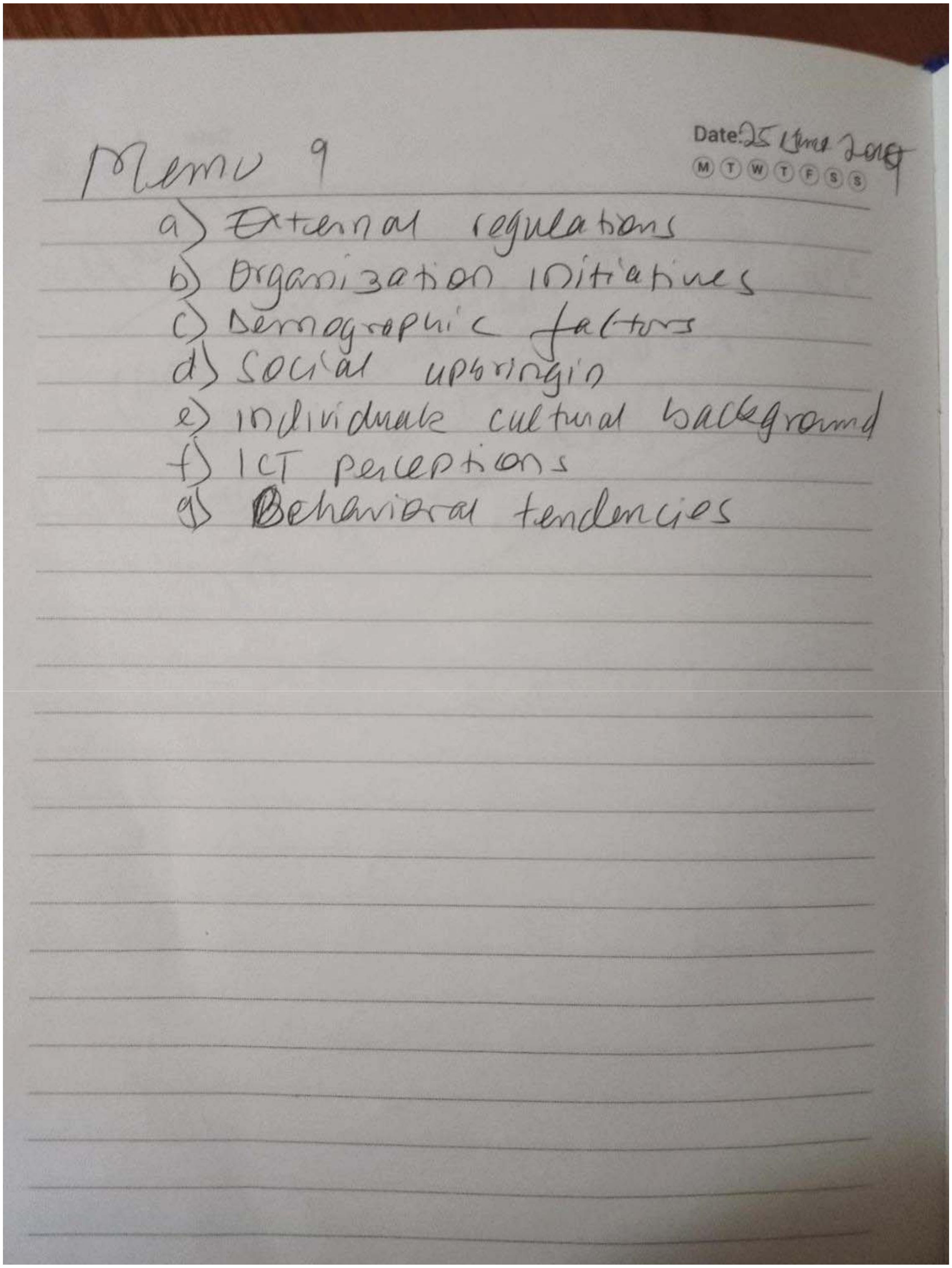
Date: 25 JUNE 2018
Ⓜ Ⓣ Ⓦ Ⓣ Ⓕ Ⓢ Ⓢ

their nature, being online and checking limits is their day to day hobby.

- Universities however found a way to mitigate this by creating programs to educate and keep the users aware of what is needed to keep safe and comply with the laid down policies.
- There was also an issue raised with students who were very bright and could try every trick on the book that they have learne in the university to attempt to compromise the university systems.

However with strong ~~to~~culture of system protection, these have not been successful.

- The categories that emerge were:



Memo 9

Date: 25 June 2019

M T W T F S S

a) External regulations

b) Organization initiatives

c) Demographic factors

d) Social upbringin

e) individuals cultural background

f) ICT perceptions

g) Behavioral tendencies

APPENDIX 12: List Journal Publications

1. **Information Security Policy Compliance: A Broad-based Literature Review and a Theoretical Framework**

Otieno E. O., Kahonge A. M., and Wausi A. N. (2019). Information Security Policy Compliance: A Broad-based Literature Review and a Theoretical Framework. *International Journal of Computer Applications* 181(47):8-13, April 2019, https://www.ijcaonline.org/archives/volume181/number47/30467-30467-2019918519

2. **Exploring the Factors That Contribute Towards Information Security Policy Compliance Culture**

Otieno E. O., Wausi A. N., Kahonge A. M. (2020). Exploring the Factors That Contribute Towards Information Security Policy Compliance Culture. *Information and Knowledge Management* 10, (5) (2020). DOI: 10.7176/IKM/10-5-05, https://iiste.org/Journals/index.php/IKM/article/view/53800

3. **A Theoretical Model for Information Security Policy Compliance Culture**

Otieno E. O., Wausi A. N., and Andrew M Kahonge. (2020) A Theoretical Model for Information Security Policy Compliance Culture. *International Journal of Applied Information Systems* 12(33):6-14, September 2020., https://www.ijais.org/archives/volume12/number33/1098-2020451879.

ce