

ADDIS ABABA UNIVERSITY

SCHOOL OF COMMERCE

DEPARTMENT OF BUSINESS ADMINSTRATION AND INFORMATION SYSTEM

BEHAVIORAL DETERMINANTS OF INFORMATION SECURITY POLICY COMPLIANCE: EVIDENCE FROM ETHSWITCH S.C

BY: BINIYAM GOSSAYE YESHITELA

ADVISOR: MESHESHA LEGESSE (PhD)

ADDIS ABABA, ETHIOPIA

APR, 2026



BEHAVIORAL DETERMINANTS OF INFORMATION SECURITY POLICY COMPLIANCE: EVIDENCE FROM ETHSWITCH S.C

By: Biniyam Gossaye Yeshitela

A Thesis Submitted to Addis Ababa University, School of Commerce in Partial Fulfillment of the Requirements for the Degree of Master of Business Information Systems

Advisor: Meshesha Legasse (PhD)

April, 2026

Addis Ababa, Ethiopia

ADDIS ABABA UNIVERSITY

Declaration

Biniyam Gossaye the undersigned, declare that this proposal entitled: "**BEHAVIORAL DETERMINANTS OF INFORMATION SECURITY POLICY COMPLIANCE: EVIDENCE FROM ETHSWITCH S.C** is my original work. I have undertaken the research work independently with the guidance and support of **Dr. Meshesha L**.

This Thesis is original and has not been submitted for any degree or diploma program in this or any other institution and all sources of materials used for the thesis has been duly acknowledged.

Name: Biniyam Gossaye Yeshitela

ID: GSE/9081/16

Signature: _____

Date: _____

Statement of Certificate

This is to certify that the thesis prepared by **Biniyam Gossaye,** entitled "**BEHAVIORAL DETERMINANTS OF INFORMATION SECURITY POLICY COMPLIANCE: EVIDENCE FROM ETHSWITCH S.C"** and submitted in partial fulfillment of the requirements for the Degree of Master of Arts in Business Information Science complies with the regulations of the University and meets the accepted standards concerning originality and quality.

Meshesha Legasse (PhD) _____ _____

Research Advisor Signature Date

ADDIS ABABA UNIVERSITY

COLLEGE OF BUSINESS AND ECONOMICS

SCHOOL OF COMMERCE

BUSINESS INFORMATION SYSTEMS PROGRAM

IMPACT OF BEHAVIOURAL FACTORS ON INFORMATION SECURITY POLICY COMPLIANCE IN FINANCIAL INSTITUTIONS: EVIDENCE FROM ETHSWITCH S.C.

By: Biniyam Gossaye

Approval of Examiners

Meshesha Legesse (PhD)

Advisor Signature

_____

Internal Examiner	Signature	Date
Hailay B. (PhD)	_____	_____

External Examiner	Signature	Date
Mehari K. (PhD)	_____	_____

AKNOWLEDGMENT

First and foremost, I want to express my gratitude to the Almighty God for His invaluable care and support that has been with me throughout my life. I also want to sincerely thank my family for their support and guidance, which has contributed to my current success. Additionally, I would like to express my deep appreciation to my advisor Dr. Meshesha Leggese, who has provided invaluable guidance and support throughout this journey. Finally, I would like to convey my deep thanks and appreciation to all my friends and colleagues for their insightful discussions and assistance during this study.

Contents

Declaration i
List of Table viii
List of Figure ix
ABREVATIONS x
Abstract xi
CHAPTER ONE 1
INTRODUCTION 1
1.1 Background of the study 1
1.2 Background of the company 4
1.3 Statement of the problem 4
1.4 Research Objective 6
1.4.1 General Objective 6
1.4.2 Specific Objective 6
1.5 Significance of the study 6
1.6 Scope 7
1.7 Definition of Terms 8
CHAPTER TWO 9
LITERATURE REVIEW 9
2.1 Definition and Evolution of Information Security 9
2.2 Information Security Policy Compliance 10
2.3 Theoretical Framework for Information Security Compliance 11
2.3.1 Theory of Planned Behaviour 11
2.4 Factors Affecting Security Policy Compliance 13
2.4.1 Behavioural Factors Affecting Security Policy Compliance 14
2.5 Challenges to Information Security Awareness and Compliance in Africa and Ethiopia 16
2.6 Extensions on TPB in security policy compliance 19
2.7 Empirical Review 20
2.8 Conceptual Framework 21
CHAPTER THREE 25
RESEARCH METHODOLOGY 25
3.1 Description of the Study Area 25
3.2 Research Approach 25
3.3 Research Design 25
3.4 Sampling Design 26
3.4.1 Population of the study 26

3.4.2 Sampling Method 26
3.4.3 Sample Size 26
3.5 Sources of Data Collection 27
3.6 Research Instruments 27
3.7 Methods of data collection 29
3.8 Procedures of data collection 29
3.9 Data analysis methods 29
3.10 Validity and Reliability 29
3.10.1 Validity 29
3.10.2 Reliability 29
3.10.3 Common Method Bias 30
3.11 Ethical Consideration 31
Research Time Schedule and Budget 32
Chapter Four 33
DATA Presentation, Analysis and Discussion 33
4.1 Introduction 33
4.2 Response Rate 33
4.3 Demographic Characteristics 33
4.4 Reliability Results and Validity Analysis 35
4.4.1 Reliability Result 35
4.4.2 Validity Analysis 35
4.5 Descriptive Statistics 39
4.5.1 Descriptive Analysis of Attitude 39
4.5.2 Descriptive Analysis of Subjective Norm 40
4.5.3 Descriptive Analysis of Perceived Behavioural Control 41
4.5.4 Descriptive Analysis of Habit 43
4.5.5 Descriptive Analysis of Regret 44
4.5.6 Descriptive Analysis of Intention 45
4.5.7 Descriptive Analysis of ISPC Behaviour 46
4.6 Inferential Analysis 47
4.6.1 Correlation Analysis 47
4.6.2 Assumption of Multiple Linear Regression 49
4.6.3 Multiple Linear Regression 56
4.7 Mediation Analysis 62
4.8 Test of Hypothesis 66
Chapter Five 72

Summary Conclusions and Recommendations 72
5.1 Conclusion 72
5.2 Theoretical Implication 73
5.3 Recommendations 75
5.4 Recommendation for Management 77
5.5 Strategic and Organizational Recommendations 78
5.6 Limitation of the study 78
5.7 Recommendation for future research 79
Reference 80
APPENDIX 87

List of Table

Table 1 Time Schedule 32
Table 2 Budget 32
Table 3 Demographic Characterstics 33
Table 4 Reliablity Result 35
Table 5 KMO and Bartlett 36
Table 6 EFA 37
Table 7 Convergent and Discriminant 38
Table 8 Attitude Descriptive Statistics 39
Table 9 Subjective Norm Descriptive Statistics 40
Table 10 Pereceived Behavioural Control Descriptive Statistics 41
Table 11 Habit Descriptive Statistics 43
Table 12 Regret Descriptive Statistics 44
Table 13 Intention Descriptive Statistics 45
Table 14 ISPC Behaviour Descriptive Statistics 46
Table 15 Correlation Analysis 47
Table 16 Model 1 Multicollinearity Test 49
Table 17 Model 2 Multicollinearity Test 53
Table 18 Model 1: Model Summary 56
Table 19 Model 1: ANOVA Test 57
Table 20 Model 1: Coefficient of predictor veriable 57
Table 21 Model 2: Model Summary 59
Table 22 Model 2: ANOVA 60
Table 23 Model 2: Coefficient of predictor variable 61
Table 24 Mediation Analysis 62
Table 25 Hyphothesis Test 70

List of Figure

Figure 1 TPB 11
Figure 2 Conceptual Framework 22
Figure 3 Harman's single-factor test 31
Figure 4 Model 1: Histogram 51
Figure 5 Model 1: P-P Plot 51
Figure 6 Model 1: Scatterplot 52
Figure 7 Model 2: Histogram 54
Figure 8 Model 2: P-P Plot 54
Figure 9 Model 2: Scatterplot 55

ABREVATIONS

TPB: Theory of Planned Behaviour

TRA: Theory of Reasoned Action

PMT: Protection Motivation Theory

VPN: Virtual Private Network

IDS: Intrusion Detection System

IPS: Intrusion Prevention System

NAC: Network Access Control

DDoS: Distributed Denial of Service

MFI: Microfinance Institutions

PSO: Payment Service Operator

PII: Payment Issuer Instrument

INSA: Information Network Security Administration

NBE: National Bank of Ethiopia

Abstract

The security technology field has made progress, yet employee conduct continues to be the most important aspect which organizations need to protect their information security policies. So, understanding what drives or limits this behavior is especially important in financial institutions where risks are high. This research study investigates how staff members' behavioral patterns impact their adherence to information security policies, using both the Planned Behavior Theory and extended additional concepts of habit formation and anticipated future regret. The researchers conducted a study using a quantitative research approach which involved both descriptive and explanatory research designs. Data were collected through a 5-point Likert-scale questionnaire adapted from prior studies. Responses were collected from 186 employees online. The data were analyzed using descriptive statistics, correlation, multiple regression, and mediation analysis in SPSS. Both attitude and perceived behavioral control directly affect compliance on both direct and indirect pathways which lead to intention, while subjective norm affects compliance through its connection with intention. Intention shows a strong effect on actual compliance behavior. Habit has a direct effect on compliance but does not influence intention, whereas regret shows no significant effect on either intention or behavior. The study demonstrates that employee abilities together with their intention to achieve designated goals determine the success of ISP compliance, whereas emotional and habitual factors have minimal impact on ISP compliance success. It extends TPB by showing that not all additional behavioral variables are equally relevant in structured organizational environments, offering practical insight for improving compliance strategies in financial institutions.

CHAPTER ONE

INTRODUCTION

1.1 Background of the study

Many organizations in most part of the world have a security problem. The problem is not usually from hackers breaking in from the outside. The problem often comes from their own workers, like employees sometimes make a mistake, as they break the rules on intentionally or unintentionally. This impact is hard in banking and finance, where institutions handle many different personal financial details, and just showing a little carelessness in following rules can lead to impactful money losses, loss of trust, and facing issue in retaining customers. Risks to information systems are serious business, and a big part of those breaches come from people inside staff or employee who already have access, not outsiders trying to break in.

Institutions have to setup a strong system in place to filter out and stop security issues, guarding the security and defending against all types of fast changing cyber-attacks and scams out there. Best ways to stop fraud depend on the latest technologies and solid habits which is behavioural factors for keeping data safe, which helps to secure financial information's and keep the company trusted with its customers then leads to retain its customer by creating confidence in security.

Defenses in a company always includes latest moder defense technologies or tools and how employee's act on these technologies or tools. Sure, things like firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Virtual Private Networks (VPN), Network Access Control (NAC), Antivirus / Anti-malware software, Secure Web Gateways and DDoS protection systems are key, but they don't work effectively alone solely without dealing with the people or employee side behavioral things. Those people-oriented steps are useful for building a conscious mindset where every employee's thinks about security, encouraging and motivating everyone to follow the rules and the policies with clear guidelines, and running knowledge serious sessions to make sure everyone knows about the risks. Right at the heart of all, this is the Information Security Policy, that is laying out the basic rules and tips to protect and secure important information, stick to laws, policies and that guide how the staff handle

things. But just only having the policy doesn't necessarily mean everyone will stick to it, which shows why it's so important to figure out what really gets people to comply (Abebe et al., 2020).

Fast payment networks around the globe go through many safety holes, with many initiated from people inside the companies rather than outsider attackers breaking in. Bahrain's BenefitPay system, that is a central national switch handling different electronic transfers within banks issues have caused from where weak spots in connections or staff handling simply let unauthorized changes slip through, that is leading to fraud issues and potential big disruptions. Problems like that often related to careless employees falling for scams or security issues, poor controls on who will accesses what, or even intentional deliberate actions from within, opening the door to breaches, fake and fraud payments, or outright system failures. Add in outdated software or lack proper monitoring, and it gets easier for these internal flaws to cause real huge damage, which is why everyone keeps pushing for better staff security awareness, strict user access rules, and ongoing checks to stop the team or employees from assumed us the biggest vulnerability (World Bank, 2025).

Ethiopia is working tirelessly to use digital payments in its financial sector, but it also opens up real worries about financial information security, and number of those risks arise from the inside employee’s rather than outsiders’ suspects. EthSwitch sits at the center of it all as the national switch connecting financial institutions such as banks, PSO’s, MFI’s, PII, through interoperability in ATM, POS terminals, mobile banking, and mobile wallets, handling huge volumes of transfers every day. Even if institutions requested to submit security checks from Information Network Security Administration (INSA), a security issue from individual institution like phishing attacks, ransomware, malware spreads, DDoS attacks, insider threats, or fraud schemes may impact the security. That kind of individual treat may arise from weak spots get exposed again and again, whether its staff getting tricked into giving away some accesses, weak controls on managing privileges, or someone deliberately causing trouble from within. Using outdated tools or weak security monitoring will end up with higher chances of financial data getting stolen, fraud transactions, or the whole network grinding to a stop, which really underscores the urgency for stronger staff employees training, tighter internal

rules, and better collaboration to close off those insider vulnerabilities (The Reporter Ethiopia, 2025).

The Information Network Security Administration (INSA) handles the major measures of cybersecurity related things in Ethiopia, drawing powers from key laws like the Information Network Security Agency Re-establishment Proclamation No. 808/2013, which shows its role in protecting critical infrastructure and dealing with threats that may harm institutions, it could come from anywhere, including also insiders' security issue. They also link into the Computer Crime Proclamation No. 958/2016, giving them tools for investigations, forensics, and preventive steps against cyber-attacks, with a focus on building mechanisms like awareness and standards to stop careless or deliberate risks from employee inside the organizations. INSA pushes for training and monitoring to make sure policies get followed, knowing human errors often lead to security issues.

At the National Bank of Ethiopia (NBE), they have rolled out directives for banks and financial institutions, such as the IT management rules for microfinance spots (MFI/33/2022), which demand solid plans for security awareness and risk handling to make sure employee stick in to policies and don't accidentally or on purpose open holes to attacks. Together, these efforts show how human behavioural aspects are key, so NBE's push for compliance checks and INSA's monitoring aim to foster habits that keep systems locked tight, especially in places like EthSwitch where there are many interoperable transactions and making one wrong security problem leads to a massive harm.

This study will examine the behavioural factors that will affect Information Security Policy Compliance (ISPC), specifically Theory of Planned Behaviour (TPB), Anticipated Regret and Habit impact on ISPC. The findings will help to get useful insight on what are the behavioural factors that strongly affect ISPC in financial sector specially in national switch and give recommendation on what to improve in order to have better employee security compliance.

1.2 Background of the company

EthSwitch, established in 2011, is a share company, and the National Switch is Owned by all banks (Private and Public) the National Bank of Ethiopia, MFIs, PIIs and PSOs. It is established mainly to provide simple, affordable, secured, and efficient e-payment infrastructure services to retail payment service providers, and through them, to end users in Ethiopia; by deploying state-of-the-art technology along with highly skilled and motivated professionals. The underling mandate of EthSwitch is contributing to the modernization of the national payments system and enhancement of financial inclusion in the country. Since 2016, it has enabled interoperability of ATMs and POS terminals operated by all banks. Currently, it is also rolling out projects to achieve interoperability of other digital payment platforms operated by all financial service providers.

It's Services

- Ethiopay – Domestic Card Scheme.
- Electronic Retail Payment Switching and Clearing.
- Hosting – Primary Switch Banks
- Central Card Printing, Personalization and Issuance.
- Dispute Management and Fraud Monitoring.
- Advisory and Training.

1.3 Statement of the problem

Current modern and contemporary technologies alone is no longer drive the information security alone. Most organizations now using recent modern and robust security technologies like those sophisticated firewalls, AI tools, zero trust architecture, cloud-native security which assumed to be essential and effective for protecting system integrity and critical financial data (Zamil et al., 2022). But, employee's compliance on the information security policy makes the technologies effective showing that human behavioural aspect is a key contributor in security performance (Khadka et al., 2025). So strong technical security infrastructures can fail if employee's compliance behaviour is not strong in national switch like Ethswitch and other financial institutions.

Insider threats risks are strong even with the advanced technologies. Around 35 % of security breaches are mostly linked to internal staffs and actors including accidental violation, misuse of access rights and data theft (Huy et al., 2025). The Nigerian bank suffering a $23.5 million loss despite holding ISO27001 certification highlights a

troubling reality on an organization can be technically "compliant" while remaining deeply vulnerable due to its employee's failure to follow security rules and policies (Fagade & Tryfonas, 2016). It clearly indicates that there is a gap between having security systems and ensuring secure human behaviour. This highlights Ethswitch needs to foster a strong compliance behaviour by ensuring that all employees understand the importance of adhering to information security policies.

The study by Shimels and Lessa (2023) gives a valuable insight on the information security maturity level within Ethiopian private banks, while this research effectively maps the procedural and organizational gaps in security implementation like inadequate policy documentation, insufficient incident management, and inconsistent risk analysis, it primarily adopts a structural and procedural lens. The study also acknowledges human-related challenges, including a lack of employee or staffs' awareness and lack of skilled professionals, yet it does not delve into the detailed behavioural impacts that influence whether employees actually comply with established information security policies (ISPs) in the companies. While Shimels and Lessa (2023) document structural deficiencies in Ethiopian banks, their procedural lens leaves an important question unanswered: even where policies exist, what psychological and behavioral forces determine whether employees actually follow them? This behavioral gap is precisely what the present study addresses. Unlike structural audits, behavioral compliance research examines the internal mechanisms attitudes, norms, perceived control, habits, and emotional anticipation that drive or inhibit daily security actions at the individual level.

The Indonesian study by Putri Maharani Akib et al. (2025) applies TPB but tests only its attitudinal component, leaving subjective norms and perceived behavioral control unexamined and limiting the model's explanatory completeness. Sommestad et al. (2019), working with 645 Swedish white-collar workers, extended TPB with habit and anticipated regret and showed these additions raised explained variance in compliance intentions yet that study was conducted in a high-income, institutionally mature Scandinavian context. Crucially, the applicability of these findings to developing-country, high-stakes financial infrastructures such as EthSwitch has never been empirically tested. This is a substantive theoretical gap, not merely a geographic one: Ethiopia's financial sector combines rapid digital transformation, a still-maturing security culture, and a highly hierarchical organizational structure conditions under

which the relative influence of habit, regret, and social norms on compliance may operate very differently than in Western settings. Existing studies on Ethiopian organizations either ignore behavioral predictors altogether (Shimels & Lessa, 2023; Abay et al., 2022) or address them only qualitatively. Moreover, no prior study has tested whether regret and habit independently explain compliance behavior beyond what intention already accounts for in this context. Therefore, this study fills a theoretically motivated and contextually specific gap by rigorously applying and testing an extended TPB framework encompassing attitude, subjective norm, perceived behavioral control, habit, and anticipated regret within Ethiopia's national payment infrastructure.

1.4 Research Objective

1.4.1 General Objective

To examine how key behavioral factors influence employees' intentions and, in turn, shape their information security policy compliance behavior.

1.4.2 Specific Objective

1. To examine the effect of TPB constructs (Attitude, Subjective Norm and Perceived Behavioural Control) and the extended variables (Habit and Regret) on employee's intention to comply with information security policy compliance.

2. To assess the influence of intention and Perceived Behavioural Control on employee's intention to comply with information security policy.

3. To analyse the mediating effect of intention between TPB constructs (Attitude, Subjective Norm and Perceived Behavioural Control) and the extended variables (Habit and Regret) with employee's information security policies compliance behaviour.

1.5 Significance of the study

Understanding the behavioural factors that really influence employees' compliance with information security policies are crucial for strengthening organizational security, particularly in Ethiopian financial sector where plenty of sensitive data is constantly at risk. This study provides insights on how TPB constructs such as attitude, subjective norms, perceived behavioral control additional extended constructs habit, and anticipated regret shape both the intention and actual compliance behaviour of

employees on policy. By highlighting these drivers, financial institutions like EthSwitch can design more effective interventions, training programs, and awareness campaigns that are planned to shape the behavioral tendencies of their staff.

Moreover, this research contributes to the academic and practical understanding of information security compliance by applying already established behavioural theories to the context of Ethiopian financial institutions. The findings can used as a reference for managers, policymakers, and researchers seeking evidence-based strategies to promote stable practices, reduce security breaches, and increase a culture of accountability. In the long term, the study helps institutions not only protect financial assets but also build trust with customers and retain those customers by demonstrating a proactive approach to information security.

1.6 Scope

Geographical and Organizational Scope

This research is focused entirely within Addis Ababa, Ethiopia. The data collection will be conducted specifically at the Ethswitch head office and two of its branches. This focus is useful because securing management permission and physical access for surveys is only feasible within these selected Addis Ababa sites, and helps keeping logistics manageable within our timeframe and budget.

Methodological Delimitation

The study will adopt a quantitative, cross-sectional research design, based on a structured questionnaire for the data collection. This means we will not use qualitative methods such as interviews, focus groups, or case study analysis. While qualitative data could offer richer narrative insights, a quantitative approach helps us to effectively gather data from a larger number of employees at the chosen sites and apply strong statistical testing the theoretical model. This choice balances depth with the practical need for generalizable findings from the sample.

Theoretical and Variable Delimitation

Our investigation is shaped by an extended Theory of Planned Behaviour (TPB) model with other additional constructs. We will focus on the core Theory of planned behaviour constructs such as Attitudes, Subjective Norms, and Perceived Behavioural Control and an integrated two additional psychological variables Regret and Habit. We have consciously chosen not to include other behavioural theories like Deterrence theory,

Protection motivation theory etc. This decision is driven by the need to keep the research model optimal scoped and testable. Adding more variables would complicate the analysis beyond the planned scope of our statistical expertise and the intended length of the employee survey.

Subject (Sample) Delimitation

The participant on the research questionnaire is strictly limited to permanent and contractual employees working at Ethswitch head office and at the branches in Addis Ababa. Since security is for all, we include all employees.

1.7 Definition of Terms

Security policy: document that spells out the rules, expectations, and overall approach that an organization uses to maintain the confidentiality, integrity, and availability of its data.

Security policy Compliance: information security compliance is the set of controls and practices a business implements to meet regulatory obligations, industry standards, and internal policies for safeguarding sensitive data, protecting IT assets, and reducing information security risk.

Theory of Planned Behaviour: is a psychological theory that links beliefs to behaviour using the three constructs Attitude, Subjective Norm and Perceived Behavioural theory.

Habit: is a routine of behaviour that is repeated regularly and tends to occur subconsciously.

Regret: is the emotion of wishing one had made a different decision in the past, because the consequences of the decision one did make were unfavourable.

CHAPTER TWO

LITERATURE REVIEW

2.1 Definition and Evolution of Information Security

Information security is commonly defined as the practice of safeguarding information's and the systems that store these information's, processes, and transmit it, with the plan of preserving confidentiality, availability, and integrity. This can go closely with established standards, like those from NIST, which mainly describe it as the protection of information and systems from unauthorized access, use, disclosure, disruption, or destruction to attain those same objectives of confidentiality, integrity, and availability (Nieles et al., 2017). Although this day's information security is closely associated with digital platforms and cyber defense, the idea itself predates the contemporary internet. In the past days of computing, the main focus was on the physical protection and access control ensuring that only the permitted individuals could interact with those sensitive data or operate critical systems. As networked communication grew up, especially with the modern developments such as ARPANET and the introduction of standardized protocols, the idea of securing information made a shift beyond physical boundaries and toward protecting data in transit aside from those physical security. New innovations like public-key cryptography further demonstrated how safeguarding information required structured, reliable mechanisms for communication and verification (Islam et al., 2025).

The advancement of information security expedited significantly as cyber threats became more complex, hard and widespread. At early 2000s, massive malware attacks and denial-of-service (DOS) incidents uncovered that simple boundary defenses were no longer adequate. So, Organizations began implementing more advanced security tools such as intrusion detection systems (IDS), stronger and standard encryptions, and coordinated incident response frameworks. This period also showed the beginning of regulatory and standards-based approaches, indicating the understanding that security should be enforced not only through latest technology but also through standard policy and oversight (Ahmad et al., 2024). Through time, the discipline enhanced from reactive measures to proactive strategies to reduce incidents, incorporating artificial intelligence (AI), automation, and continuous monitoring to predict and mitigate risks rather than solely responding after incidents occur.

More recent researches emphasizes that information security is not solely a technical pursuit, but also a compressive one influenced by standard policy, management, and human behavioral aspects. Modern perspectives recognize that effective protection requires unified strategies that can address both technological and organizational dimensions. Issues like awareness, compliance, and policy consistency have become core to sustaining secure environments, underscoring that the information security must evolve beside changing technologies and threat landscapes (Ganapati et al., 2023).

Taken together, the progression of information security reflects a stable progression from different separated system protection to complex ones, interconnected defense strategies. Its progress shows that a shift from simple access control to comprehensive complex frameworks that merge technology, policy, and human behavioral factors like attitude, subjective norm, perceived behavioral control, regret and habit. This ongoing transformation shows that securing information is not a final stage but, it is also an ongoing effort that adapts to recent technologies, emerging threats, and the growing dependence on digital systems.

2.2 Information Security Policy Compliance

Information security policy compliance (ISPC) really comes down to employees and organizations actually following the accepted guidelines to protect information and systems from different kinds of attacks. Bulgurcu et al. (2010) examine this through a rational lens, showing how people's or employee’s intentions to comply are shaped by considering the advantages like keeping the resources safe or potential rewards counter to costs, such as work disruption or the risks and penalties from not complying. The study links this directly to the information security awareness, noting that better understanding of the results helps form a positive attitude toward following the policy, with added elevates from social norms among colleagues or coworker and personal confidence in handling security tasks. Finally, it's about shifting compliance into a logical and rational choice that feels beneficial on all daily tasks.

When examining different industry sector, the way compliance is tackled shifts because each sector faces its own kind of different risks and needs. Mishra et al. (2022) evaluates cybersecurity policies in areas like healthcare, finance, education, aviation, and e-

2.3 Theoretical Framework for Information Security Compliance

There are many different behavioural theories that is developed to understand and predict Information Security Policy Compliance (ISP). From those we will focus on Theory of Planned Behaviour (TPB).

2.3.1 Theory of Planned Behaviour

The Theory of Planned Behaviour (TPB) is a strong psychological framework developed to predict and elaborate human behaviours in specific contexts. It functions as an expansion of the theory of reasoned action (TRA) that was developed earlier the development of TPB, specifically addressing situations where individuals may lack complete intentional control over their actions. According to Ajezen et al. (1991), an individual's behavioural achievement is primarily motivated by their intention to that behavior, which is itself determined by three independent factors or constructs: that is their personal attitude towards the behaviour, subjective norms showing social pressure, and perceived behavioural control.

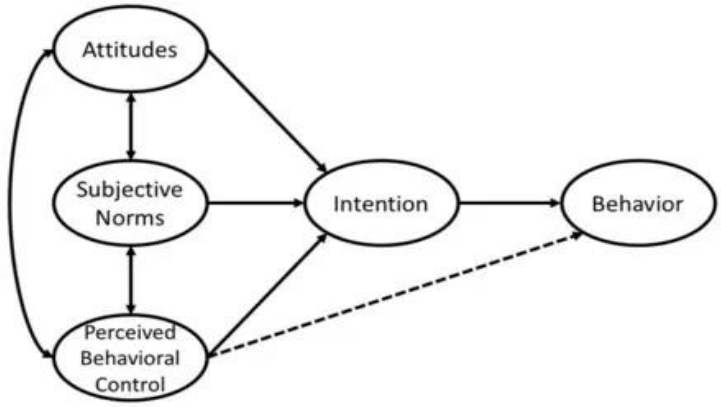


Figure 1 TPB

Based on the comparative evidence presented by Nasir et al. (2018), the Theory of Planned Behaviour (TPB) remains the most fitting framework for assessing information security policy compliance when compared with other behavioural theories like PMT, deterrence and others. Unlike General Deterrence Theory and Protection Motivation Theory, TPB regularly shows stronger and more stable explanatory power using its core constructs attitude, subjective norms, and perceived behavioural control which have frequently shown significant relationships with both intentions to comply and compliance behaviour.

PMT, for instance, has been one of the most widely applied theories in this field. A recent systematic review by Liang et al. (2021) covering over a decade of PMT-based security studies found that threat and coping appraisals strongly predicted security intentions, particularly in contexts where employees could clearly picture the personal consequences of a breach. General Deterrence Theory has also been applied extensively, and a meta-analysis by Bauer and Bernroider (2017), updated in later work, found that sanctions do reduce non-compliant behavior but importantly, their effect is much stronger in cultures with high power distance and where enforcement is visible and consistent. This is actually a significant point for the Ethiopian context, since the presence of hierarchical authority at EthSwitch might amplify deterrence effects in ways not captured by TPB alone. Neutralization Theory adds yet another layer, explaining why employees who genuinely know the rules still choose to break them by convincing themselves that "no real harm is done" or "it was necessary" techniques that Vance et al. (2020) showed remain active and predictable even in formal organizational settings. What all these frameworks share, though, is that each only captures part of the picture: PMT focuses on threat, deterrence on punishment, neutralization on rationalization. None of them accounts for social pressure, perceived capability, habitual routine, and emotional anticipation at the same time. That combined explanatory power is precisely what the extended TPB model in this study offers, and that is the argument that should anchor the theory section.

TPB is a theory of behavior that explains human behavior as a result of an individual's intention to perform a behavior which in turn is predicted by three aspects of behavior: attitude, subjective norms and perceived behavioral control. In EthSwitch’s target environment of managed businesses where peer pressure and a host of organizational and other factors influence employee behavior, TPB offers a better psychosocial explanation of secure behavior determinants than models such as PMT that focus on threat/reward appraisals, or Deterrence Theory that focus on sanctions. Empirical studies within organizational environments have found the TPB constructs to be very effective predictors of secure behavior intentions and actual behaviors. Security culture deserves its own mention here because it operates at a different level of analysis from typical TPB-style behavioral models. In a widely cited review of 58 studies, Uchendu et al. (2021) describe security culture as the shared values, norms, and behavioral expectations around cybersecurity within an organization. Rather than directly

predicting individual decisions, it shapes the broader environment in which those decisions are made. In other words, culture sets the stage, but it is the individual psychological variables that determine what happens on it. For this reason, security culture in this study is treated as a relevant contextual backdrop particularly important given that EthSwitch is a relatively young institution operating in a rapidly digitizing financial sector rather than a competing theoretical framework.

2.4 Factors Affecting Security Policy Compliance

Factors affecting information security policy compliance often spin around the organizational elements that either promote or impede employees from sticking to the rules, regulations or policies developed by the organization. On the study applied on a public telecom company in Ethiopia, Assefa et al. (2021) indicates that management support is a critical, where leaders who actively back security initiatives make the staff more likely to follow the policies because employees see security compliance as a priority when it comes from the top. They also identified that awareness and training programs are the key, as these help staff to understand the security risks and how to manage those risks, turning most policies into practical habits that reduce accidental breaks or loop holes. Liability rounds out their observation, with explicit consequences for non-compliance pushing staffs to take ownership, though the study notes this works best in organized environments like large public institutions where policies are already positioned but enforcement varies.

On a wider empirical level, Alzahrani (2021) investigates or shows into how individual and colleague related issues impact compliance, exhibiting or showing that things like security system anxiety where users feel overwhelmed if there are a complex security tools and can actually hinder them make them resistant from following policies, as the focus leads to avoidance. Non-compliant behaviours from staff members also reduce overall employees compliance behaviour that is creating a kind of visible effect where seeing other employees break the rules and normalizes it, while work barriers, surprisingly, can boost intentions to comply if they're seen as necessary hurdles that protect the bigger picture. The research emphasizes security visibility as a constructive force, making policies more noticeable, applicable and thus easier to follow, and links in security education systems as a way to ease those barriers through better preparation.

In the context of Ethiopian banks facing the cyber threats, (Aimero 2023) stress how external factors like frequent attacks expose gaps in compliance, with factors such as insufficient training and also resource limitations directly influencing how well the staff adhere to security protocols and policies during incidents. The study also shows that a lack of regular security awareness programs makes employees vulnerable to different kinds of internal and external attacks, this indirectly lowering the compliance rates as they battle without proper guidance. It also touches an organizational culture, where weak execution from management boosts non-compliance, especially in critical sectors like finance sectors where breaches or loop holes can have huge negative implications, underscoring the need for tailored and structured strategies to build resilience against these influences.

2.4.1 Behavioural Factors Affecting Security Policy Compliance

When we think of behavioural factors in information security policy compliance (ISPC), the TPB stands out as a best framework that includes personal attitudes, subjective norm (social pressures), and perceived behavioural control (sense of control to how people actually follow security rules). Alshammari et al. (2025) put this into practice by combining TPB with other behavioural theories like operant conditioning and protection motivation, and it shows how attitude toward behaviour affects, whether someone assumes complying as a good idea and what is the impact of colleague compliant action along with perceived behavioural control, like feeling capable of doing what is required, directly increases intentions to stick with information security policies. The study found these behavioural elements notably shape employees' mindset in actual context, where positive views and confidence in managing tasks lead to stronger commitment towards information security policy, though things like subjective norms from colleagues didn't always pack the same impact. This inconsistency in how subjective norms perform across studies is actually one of the more interesting patterns in this literature, and it deserves more than a passing mention. Bulgurcu et al. (2010) found subjective norms to be significant in a Turkish organizational sample, while in Alshammari's (2025) study they were not. A study by Moody et al. (2018), which developed and tested a unified model of information security policy compliance across different contexts, showed that the strength of normative influence can vary considerably depending on the level of hierarchy in the organization. In more

centralized and hierarchical environments, where authority and directives flow clearly from the top, employees often comply primarily out of deference to leadership rather than peer pressure. As a result, the subjective norm construct appears to capture a somewhat different underlying mechanism than it does in flatter, more collaborative organizational settings.

This matters directly for EthSwitch. As a nationally regulated financial infrastructure with a clear chain of command, the source of normative pressure is likely managerial authority rather than colleague influence — and standard TPB subjective norm items, which ask about "what others think I should do," may not fully capture that. Testing this empirically in the Ethiopian context is therefore not just a replication exercise; it adds something genuinely new to what the literature currently knows.

The systematic reviews, Delso-Vicente et al. (2025) indicates TPB as one of the trusted theories for unpacking why employees comply or violate information security policy, demonstrating that intentions driven by attitudes, subjective norms, and perceived behavioural control are crucial in combining human behavior with technology defenses. They point to empirical work where theory of planned behaviour helps explain compliance through factors like personal responsibility and organizational support, noting that when people feel their actions are really align with what is anticipated socially and they have the tools to act using the three constructs to improve compliance. This approach links or fills the gap between individual mindset and wider cultural influences, showing that behavioural models like TPB are crucial for crafting strategies that go beyond tech fixes to address the human side of security lapses.

On the wider scale, Almansoori et al. (2023) in their review of cybersecurity behaviour studies observe TPB appears in various key investigations, often bridging subjective norms such as influence from peers and attitudes to intentions that drive secure actions. They observed TPB being used beside theories like protection motivation theory to explore how perceived control over human behaviours affects compliance in an institutional context, with results clearly suggesting that when people believe they can handle information security tasks without much hassle, they're more likely to follow it through. This emphasizes the role of TPB's in showing preventable gaps, like low confidence leading to risky shortcuts, and pushes for tailored interventions that build on these behavioural insights to encourage better policy compliance overall.

2.5 Challenges to Information Security Awareness and Compliance in Africa and Ethiopia

In the Ethiopian banking sector, one of the biggest obstacles to strong information security comes from gaps in how well employees understand and follow standard security policies, often linked with wider organizational and cultural issues. Woretaw et al. (2019) examined carefully at banks in Addis Ababa and found that while many have basic security policies in place, the overall security culture is weak, with employees not fully holding the risks from things like weak password habits or sharing sensitive data easily. They showed that without a regular training and clear leadership support, employees tend to overlook threats, leading to higher chances of breaches in a system that is increasingly linked but not always protected. This includes into larger Sub-Saharan trends were low awareness stems from unequal technology adoption, making it hard for banks to keep up with evolving cyber risks.

When it comes to particular technology like banking cards, compliance with global standards indicates even more cracks in Ethiopian practices. Lessa et al. (2023) checked how well local financial institutions stack up against PCI-DSS requirements and found that major areas, such as network security and access controls, fall short, often due to outdated systems or inconsistent monitoring. Their survey of IT revealed that while some essentials like firewalls are there, things like usual vulnerability scans and proper encryption aren't fully implemented, which exposes cards data to attacks or hackers. This is not just only a technology fix, it is about developing routines where staff regularly check for weaknesses, but in Ethiopia's context, the limited resources and lack of training drag that back, echoing problems across African financial sectors where rapid digital growth outpaces security measures.

Looking broader to Sub-Saharan Africa, places like Nigeria, behavioural and social factors play a key role in why awareness and compliance are lagging. Nasir et al. (2020) explored SMEs in Nigeria and showed how cultural norms, like informal data sharing habits, conflict with strict security needs, leading to low adherence even when security policies exist. They proposed that without addressing these human behavioural elements through targeted interviews and case studies, organizations are at high risk and ongoing vulnerabilities, much like in Ethiopian banks where similar low literacy levels and high technological costs compound the issue. This points to a need for

customized approaches that consider local contexts, rather than just importing foreign standards.

Across Africa, a review of studies highlights that human errors and policy gaps are common responsible factors behind the security beaches. Lubua et al. (2021) integrated research from the continent and mentioned that factors like insufficient training programs and over trust among colleagues often lead to security breaches, with women sometimes facing higher risks due to gender dynamics in technology roles. In Ethiopian banking, this aligns with findings where work environments lacking clear accountability increase threats, suggesting that enhancing awareness through ongoing education could help link these gaps and foster a more secure financial landscape.

An interesting but also neglected factor is the aspect of habit. In their examination of factors influencing personnel compliance with IS security policy issues, Nord et al(2020) pointed out that repeat behaviours by employees, occurring without consciously thinking about them, such as logging into the system daily or following certain security procedures in an automated manner without consciously considering it, may be significantly influenced by habit. Based on this, the study revealed that exceeding habit particularly enhanced employee's control in regard to IS security policy compliance.
If these aspects are generalised to other industries, then what does it mean for the Ethiopian setting. With financial institutions in Ethiopia, Employees still rely on formal training and documentation, while yet at the same time falling back to their old habits, once the initial training fades away.

However, if for the authors', habit actually is the key for holistic internalisation of IS security behaviours, then how organizations attempt for sustainable compliance should use approaches to reinforce these habits instead of only attempting awareness once and not again. As well using re-enforcement strategies such as repeated drills or gradually nudging behaviours with low-impact activities such as from simple daily login reminders to the security-related menu system as examples, to induce these behaviours in an automatic manner. Based on the authors' findings, an extract from this conclusion relates to the fact that however younger generations or staff with little IT knowledge or awareness may also need additional training of their own in order to develop these very

same habits, which the authors found that differences between age, gender and level of awareness were found to be highly significant. Therefore, new strategies must be adopted to indigenous literature, to develop these fundamental and beneficial addiction in any given organisation in the country. The interesting theoretical tension here is that if habit works automatically below the level of conscious thought, then it may not operate through intention at all. A 2023 study by Weickert et al. published in Computers & Security examined the habit-intention gap in cybersecurity contexts and argued that well-established security routines can strongly predict actual behavior even when intention scores are low or unstable. This finding challenges the core assumption of the Theory of Planned Behavior (TPB) that intention is always the critical mediating step between attitudes and actual compliance. In a workplace like EthSwitch, where employees repeat the same login procedures, access protocols, and device-handling routines many times a day, some of those behaviors have almost certainly become automatic. Measuring whether habit predicts compliance independently or whether it works through intention is therefore a genuinely important empirical question for this study to answer, not just a box to check.

Another factor influencing a security policy compliance is an anticipated regret which Kuppusamy et al. (2022) defined as the uneasy feeling employees expect to experience or feel when they imagine the experience of having a particular outcome that could have been avoided occurred. Evidence shows that in the where this variable is included, the expectation of having that undesirable event take place is positively related to compliance intention. Anticipated regret may be particularly important in the Ethiopia context, in light of the emerging digital economy where many organizations are still trying to establish their security practices to contend with the evolving cyber threats. The employees who can picture in their mind the costly aftermath of the data breach caused by their own actions no doubt feel even more compelled to follow the policy. This sentiment can be useful in strengthening the security policy compliance in Ethiopian companies. A 2024 study by Chen et al., published in Chinese Management Studies, found that anticipated regret significantly influences workplace safety compliance, and that this relationship is substantially shaped by the organization's ethical climate. This suggests that regret does not operate uniformly across all settings its effectiveness depends heavily on the broader ethical environment employees

experience. Specifically, in workplaces characterized by an egoistic ethical climate where self-interest dominates and collective responsibility is weak the effect of anticipated regret on compliance was noticeably diminished. This finding has a direct bearing on the current study. At EthSwitch, where compliance is largely rule-based and monitored from the top down rather than driven by individual moral judgment, the ethical climate may not be the kind that amplifies personal regret. Employees may experience low psychological ownership over security decisions, which would reduce the emotional salience of anticipated regret and explain why it may fail to predict compliance intention in this specific context. Testing this empirically is therefore one of the more interesting theoretical contributions this study can make not just confirming or rejecting regret as a predictor, but illuminating the conditions under which it does and does not operate in a developing-country, high-structure financial institution.

2.6 Extensions on TPB in security policy compliance

In their 2019 study, Sommestad, Karlzén, and Hallberg examined closely into whether the Theory of Planned Behaviour (TPB) really includes all the bases for explaining why people follow information security policies. They started with the main idea that TPB's core constructs attitudes, perceived norms, and perceived behavioural control drive intentions to comply, but there's often a segment of unexplained variance, around one-third. To check the "sufficiency assumption" that nothing is missing, they collected data from a random sample of 645 Swedish white-collar workers and tested number of probable extensions. Anticipated regret is that gut feeling of future guilt if you do not comply and things go wrong, while habit refers to those automatic patterns built from the past behaviour. When added separately after the standard TPB factors in a hierarchical regression, regret raised the explained variance in intentions by 3.4 percentage points, and habit by 2.6 points small but telling improvements that suggest TPB is not fully complete for this context.

What is most noticeable is how these additions connected directly to intentions and overall actual compliance. Regret adds an emotional layer, making people exhibiting a greater tendency to intend to follow policies to avoid that nagging "what if" later on, which links to attitudes and norms by pulling some of their predictive weight. Habit, meanwhile, illustrates the non-deliberate part of security behaviours, like locking screen without thinking, and it reinforces intentions when positive routines experiences

are in place. Together, the two added extensions pushed the variance up by 5.4 points, showing that they work well together. The authors emphasize that while TPB is solid for planned actions, security compliance often involves repetitive tasks where habits dominate, and regret helps explain the motivational push. This challenges the theory's sufficiency, indicating that for real-world policy adherence, folding in these factors could make predictions to the point and more practical for organizations dealing with human problems.

2.7 Empirical Review

Getting into the empirical review of information security policy compliance, many different studies have examined behavioural factors through already established theories like the Theory of Planned Behaviour (TPB), with the additional extensions such as regret and habit proving particularly insightful, especially in financial sector. For instance, Sommestad et al. (2015) carried out a questionnaire-based survey with 306 respondents from a Swedish research organization, using hierarchical regression to assess Theory of Planned Behaviour (TPB) sufficiency. Their findings showed that adding anticipated regret referred to the emotional expectation of regret from non-compliance beside threat appraisal from PMT, considerably improved predictions of compliance intentions, explaining an additional variance that warranted model modification for security contexts. This empirical evidence tells how regret acts as a motivational force, encouraging individuals towards a policy adherence by boosting the perceived emotional costs of violation. Similarly, Sommestad et al. (2019) elaborated this in a larger sample of 645 Swedish white-collar workers, where hierarchical regressions showed anticipated regret strengthening explained variance in intentions by 3.4 percentage points individually, and habit representing established routines like automatic security checks adding 2.6 points, with a total of 5.4 points. These results empirically challenge the Theory of planned sufficiency assumption, by emphasizing habit's role in turning random deliberate intentions into steady compliance behaviours, which is essential for financial settings where repetitive tasks dominate daily operations.

Based on these insights, empirical works in Ethiopian financial institutions reflects the importance of behavioural factors in policy compliance, while reviews reinforce the need for TPB extensions like regret and habit to address gaps in security maturity and vulnerability. Shimels and Lessa (2023) examined information systems security

maturity in selected private Ethiopian banks using the SSE-CMM model and ISO/IEC 27001 controls, and finds an average maturity level of 2 (repeatable but intuitive), with discrepancies in processes like vulnerability assessment and monitoring. Their questionnaire data collected from 93 respondents signalled to challenges like lack of awareness and lack of skilled professionals, empirically connecting low adherence to behavioural flaws that could be mitigated by habit creating routines and regret related motivations. Abay et al. (2022) qualitatively analysed a case bank in Ethiopia through interviews and different document reviews, detecting gaps in vulnerability evaluation procedures and improvement, with challenges such as unfavourable managerial perceptions and unskilled staff obstructing compliance, this empirically suggests that integrating and habit could improve policy compliance in resource restricted financial environments. Almansoori et al. (2023), in a systematic review on 39 studies from 2012-2021, found that Protection Motivation Theory dominating but noted TPB's frequent use specially for compliance intentions, with 56% of studies at the organizational level showing individual level additional extensions like habit and regret are unexamined, yet vital for socially focused societies like Ethiopia. Hwang et al. (2025) surveyed 526 employees across different industries, indicating policy awareness elevates threat perception and compliance, regulated by fits like task and technology alignment, which empirically aligns with how habit actually reinforces routines in financial technology focused contexts. Alqahtani and Braun (2021) reviewed UTAUT2 elements, empirically summarizing that habit actually influences compliance behaviours, aligning TPB extensions and promoting for frameworks that integrate habit and regret to reduce security breaches in financial institutions like EthSwitch, where behavioural factors could empirically drive better policy outcomes.

2.8 Conceptual Framework

Drawing from the reviewed literature and empirical evidence, the conceptual framework presented in the figure illustrates how the key elements are interconnected and brings together constructs from multiple theoretical perspectives.

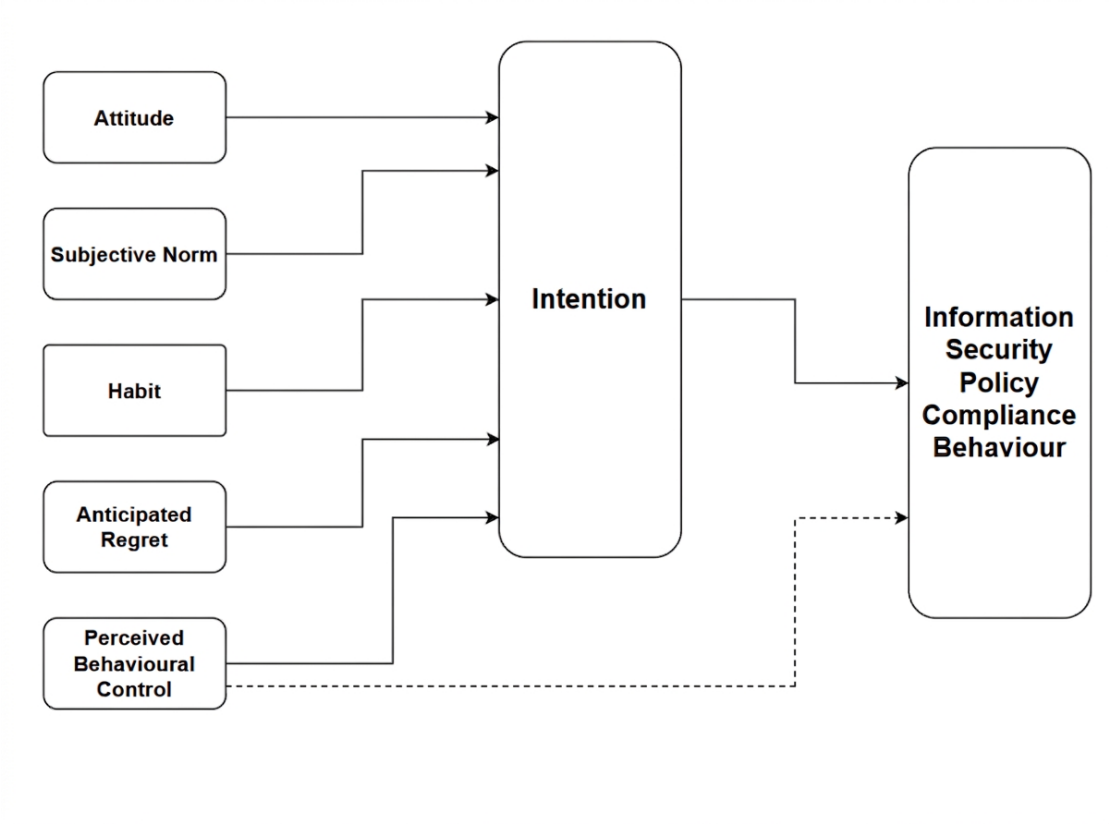


Figure 2 Conceptual Framework

Independent Variables

TPB Constructs: The study will measure the effect of TPB (Attitude, Subjective Norm and Perceived Behavioural control) on employee information security policy compliance.

Habit: The study will measure the effect of habit on employee information security policy compliance.

Regret: The study will measure the effect of regret on employee information security policy compliance.

Dependent Variable

Actual Compliance Behaviour:

The dependent variable will be the outcome that is measured by the effect of the independent variables. In this study, the dependent variable is actual employee's compliance behaviour.

Mediating Variable

Intention: will mediate the relationship between the TPB (Attitude, Subjective norm, Perceived behavioral control), regret, habit and information security policy compliance behaviour.

Hypotheses

H1: Attitude has a significant positive effect on employee's intention to comply with information security policy.

When employee's understand information security policy in a positive way, they are more likely to have intention to comply with information security policy. (Infinedo ,2011) Stated that having positive attitude will make the behavioral intention to comply to information security policy compliance stronger.

H2: Subjective norm has a significant positive effect on employee's intention to comply with information security policy.

Employee's perception or view of the social pressure from colleagues, managers or higher officials on following the information security policy policies significantly influence intention to comply with these policies Bulgurcu et al. (2010).

H3: Perceived behavioural control has a significant positive effect on employee's intention to comply with information security policy.

Employees who feel really confident in their potential to comply with information security policies are more likely to form robust intentions to do so. earlier studies show that when individuals perceive greater control over performing security related tasks like having the necessary skills, resources, and knowledge their intention to comply is improved, also increasing the likelihood of consistent policy adherence in practice (Ajzen, 1991; Ifinedo et al., 2011).

H4: Habit has a significant positive effect on employee's intention to comply with information security policy.

Sommestad et al. (2019) implied that habit applies a strong direct influence on employees' intentions to really comply with information security policies, that is leading to more stable actual compliance as these secure practices turn into automatic routines that guide behavior reliably.

H5: Regret has a significant positive effect on employee's intention to comply with information security policy.

Employees' expectation of regret plays an important role in forming their intention to comply with the standard information security policies, which subsequently affects actual compliance behaviour. Former research implies that when employees have the negative feelings they may experience after breaking security policies like guilt or self-blame they are more likely to develop a stronger intention to act accordingly (Siponen et al., 2022). This anticipated regret motivates random deliberate decision-making, solidifying behavioural intention and then in turn, promoting consistent adherence to information security requirements in everyday work practices.

H6: Intention has a significant positive effect on employee's information security policy compliance behavior.

Intention is an immediate antecedent of behaviour according to TPB. Alshammari (2025) Showed that employee's intention is positively related with the information security policy compliance. Once employees develop a robust intention to comply most likely they will follow that intention.

H7: Perceived Behavioral Control has a significant positive effect on employee's information security policy behavior.

In addition to indirect mediation effect through intention PBC has also a direct effect on Information security policy compliance behavior (Alshammari 2025). This shows a partial mediation between PBC and Compliance behavior.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Description of the Study Area

The study focusses on Ethswitch which is the biggest national switch in Ethiopia, which facilitate digital environment in the country. The company created interoperable and shared environment in Ethiopia, which is heavily relayed in the technology and information. This context provides a strong foundation for analyzing behavioural factors that lead to information security policy non-compliance at EthSwitch, encompassing both internal and external behavioral influences.

3.2 Research Approach

This study applied a quantitative research approach to examine how behavioral factors shape compliance with information security policies at EthSwitch. The goal is to objectively measure the strength of relationships between key behavioural constructs and information security policy compliance behaviour. To achieve this, the researched collected numerical data through a structured survey distributed to employees. The survey used standardized scales to measure their attitudes, perceived social pressures, and sense of control over compliance (based on the Theory of Planned Behavior), alongside their habits and fear of regret related to security practices.

By utilizing structured survey instruments, the study generates quantitative data that can be subjected to statistical analysis to identify regression, correlations, and behavioural trends among employees. Moreover, the quantitative approach supports data collection from a relatively large sample, enhancing the generalizability of the results.

3.3 Research Design

The design of this research is both descriptive and explanatory. Descriptive research serves to summarize the current levels of information security policy (ISP) compliance, as well as the prevalence of behavioral factors such as attitudes, subjective norms, perceived behavioral control (from TPB), anticipated regret, and habit among employees at EthSwitch. This component is crucial as it establishes a baseline understanding of the existing state of compliance behaviors and the influence of these

factors within the organization, highlighting patterns in a critical financial institution context.

The explanatory component enables the study to investigate why these behavioral factors affect ISP compliance, through testing hypotheses on causal relationships and exploring mechanisms like the role of regret in deterring violations or habit in automating compliant actions.

By integrating descriptive and explanatory elements, the study provides a comprehensive view of employee behavior toward information security policies, facilitating both an overview of current practices and insights into underlying drivers.

3.4 Sampling Design

3.4.1 Population of the study

The target population of this study was all workers who works at Ethswitch. There are Contract and Permanent employees at Ethsiwtch. Currently There are around 206 employees at Ethswitch. In this study, the census survey method was used. So, all technical and non-technical employees will be population of the study. Since census survey used no sampling technique was required.

3.4.2 Sampling Method

Given that a census survey was conducted, there is no need for sampling methods typically used in other studies. A census approach involves collecting data from every member of the population, thereby eliminating sampling errors and ensuring comprehensive data collection from all relevant stakeholders.

3.4.3 Sample Size

A census approach was initially employed targeting all 206 employees. However, 186 valid responses were collected, yielding a response rate of 90.3%. There were 9 contract employees recruited for urgent compilation of projects. They finish their contract before this data collection. 6 employees were abroad the country for emerging projects (IPS Use cases) training and workshop on the period of the collection. 5 employees leave the company (Turnover). The analysis was therefore conducted based on the obtained responses.

3.5 Sources of Data Collection

This research extensively examines the Behavioral Factors Influencing Information Security Policy Compliance in Financial Institutions: Evidence from EthSwitch through primary and secondary data sources.

Primary data can be defined as the original data collected directly the employees. This includes information that has been acquired from questionnaire. This technique offers first-hand impressions and elaborate particulars of the experiences and viewpoints of employees. So, the input from all technical and non-technical will be used as a primary data source.

Secondary data will be gathered from books, online databases, and scholarly publications. Secondary data were gathered from several sources, including books, online databases, and scholarly publications. It serves to support and enrich the primary data in so many ways. Thus, applying both primary and secondary data allowed for an in-depth and multidimensional analysis.

3.6 Research Instruments

The data gathering instruments for the study is very essential for collecting useful and relevant information that will help to reach out the research questions regarding the behavioral factors on Information security policy compliance. The primary data collection instrument was a structured questionnaire composed of validated scales drawn from the existing literature. Specifically, the Attitude, Subjective Norm, Perceived Behavioral Control, Intention and Compliance behaviour items were adapted from (Alshammari 2025). The Habit scale was adapted from Vance et.al (2012), and and the Anticipated Regret scale was adapted from Brehaut et.al (2003). This instrument is designed to capture quantitative data on behavioral factors influencing information security policy compliance. All items were originally formulated on a 5-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree). Minor wording adjustments were made to fit the EthSwitch organizational context without altering the semantic meaning of the original items. The questionnaire have two parts, the first part contains demographic information about a respondent, such as age, gender, and education level. This part will be useful for knowing the background of the respondents and how their different demographic information will affect their behavior and the constructs. The second part consist close-ended questions that will focus on the constructs of the behavioral aspects on complying the information security policy

compliance. Before the main data collection, a pilot study was conducted to assess the reliability and internal consistency of the adapted measurement scales. The pilot sample consisted of 21 EthSwitch employees who were not included in the final data collection. Cronbach's alpha coefficients were computed for each construct. All constructs returned alpha values above 0.70, confirming acceptable internal consistency. In addition, variance inflation factors (VIF) were examined to detect any multicollinearity among items. All VIF values were below 5, indicating no problematic collinearity. Based on these pilot results, no items were dropped or substantially modified prior to the main survey administration.

3.6.1 Reliability

Variables	No. of Items	Cronbach Alpha	Interpretation
Attitude	5	0.768	Acceptable
Subjective Norm	5	0.837	Good
Perceived Behavioural Control	5	0.883	Acceptable
Intention	5	0.959	Excellent
Habit	5	0.798	Good
Regret	5	0.747	Good
Compliance Behaviour	5	0.899	Excellent

Table 1 Pilot Reliablity

3.6.2 Multicollinearity

Coefficients[a]			
Model		Collinearity Statistics	
		Tolerance	VIF
1	(Constant)		
	PBC	0.907	1.103
	Att	0.871	1.148
	SN	0.891	1.122
	Hab	0.803	1.245
	Reg	0.898	1.113
a. Dependent Variable: Int			

Table 2 Model 1 pilot multicollinearity

Coefficients[a]			
Model		Collinearity Statistics	
		Tolerance	VIF
1	(Constant)		
	PBC	0.728	1.373
	Int	0.728	1.373
a. Dependent Variable: Act			

Table 3 Model 2 Pilot multicollinearity

3.7 Methods of data collection

The questionnaire data for this research was collected online. Google form was prepared for the data collection. This google form is preferred by its ease of use and quick setup, real-time data collection and integration, accessibility and distribution and suitability for census.

3.8 Procedures of data collection

Participants informed about the purpose of the study being conducted and they got assured that their response is confidential in order to make them confident and to make the responses genuine. The questionnaire will be distributed to the respondents via google form.

3.9 Data analysis methods

The data was coded, tabulated and clearly checked to make the data good for analysis. Quantitative data was gathered from questionnaires completed by employees. The data analyzed analyzed using SPSS version 27. The analysis includes calculating means and standard deviations, and used to assess correlations and perform multiple linear regression. So based on the analysis recommendation given to improve employee's behavior in complying with information security policy compliance.

3.10 Validity and Reliability

3.10.1 Validity

Validity measures how accurately a tool assesses the concept it is intended to evaluate. As stated by Creswell (2014), validity concerns whether the research instruments genuinely reflect the phenomena under study. To enhance the validity the questionnaires will be reviewed and assessed by the security experts. Valuable insight and clarity will be gained from them. Any research instrument must have validity check in order to measure the constructs going to be evaluated. Several techniques will be used to establish the validity of the survey instrument in this proposal on behavioral factors on information security policy compliance. A small group data will be used as a pilot testing to check the validity and to find any ambiguities or problems with the questionnaire.

3.10.2 Reliability

Reliability is a critical aspect of evaluating research instruments, ensuring that the tools used to assess constructs such as attitudes, skills, and knowledge yield consistent and

dependable outcomes (Ahmad et al., 2024), reliability indicates whether a measurement produces consistent results across different instances. When multiple attempts to measure something yield the same result, the measure is considered reliable. The most common alpha values are the rule of thumbs: Excellent ($\alpha \geq 0.9$), Good ($0.9 > \alpha \geq 0.8$), Acceptable $0.8 > \alpha \geq 0.7$), Questionable ($0.7 > \alpha \geq 0.6$), Poor ($0.6 > \alpha \geq 0.5$) and Unacceptable ($0.5 > \alpha$) (Izah et al., 2024). This study indicates that the reliability test will display suitable coefficients for both the overall scale and particular characteristics.

3.10.3 Common Method Bias

Since all variables in this study were collected from the same respondents using a single self-reported questionnaire at one point in time, the potential for common method bias (CMB) was acknowledged and addressed. To minimize this risk at the design stage, the questionnaire was structured so that the dependent variable items (compliance behavior) were separated from the predictor variable items by several intervening sections, reducing the cognitive salience of any direct association between them. Respondents were also assured of full anonymity, which reduces social desirability bias and encourages honest responses (Podsakoff et al., 2003). Following data collection, Harman's single-factor test was performed to statistically assess CMB. All items were entered into an exploratory factor analysis without rotation. The results showed that the first factor accounted for 36.803% of the total variance, which is well below the 50% threshold recommended by Podsakoff et al. (2003), indicating that common method bias is unlikely to be a serious concern in this dataset.

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings[a]
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total
1	12.881	36.803	36.803	12.881	36.803	36.803	7.458
2	2.573	7.351	44.154	2.573	7.351	44.154	9.414
3	1.947	5.562	49.716	1.947	5.562	49.716	6.545
4	1.794	5.126	54.842	1.794	5.126	54.842	7.319
5	1.462	4.177	59.019	1.462	4.177	59.019	6.506
6	1.002	2.862	61.882	1.002	2.862	61.882	6.493
7	.909	2.598	64.479	.909	2.598	64.479	8.022
8	.858	2.450	66.930				
9	.770	2.200	69.130				
10	.747	2.136	71.266				
11	.721	2.060	73.325				
12	.661	1.889	75.215				
13	.649	1.855	77.070				
14	.614	1.756	78.825				
15	.565	1.614	80.440				
16	.559	1.597	82.037				
17	.533	1.524	83.561				
18	.497	1.420	84.981				
19	.473	1.352	86.333				
20	.462	1.319	87.652				
21	.438	1.250	88.902				
22	.398	1.137	90.039				
23	.395	1.129	91.168				
24	.387	1.107	92.275				
25	.368	1.051	93.326				
26	.328	.936	94.262				
27	.303	.866	95.128				
28	.284	.812	95.940				
29	.271	.775	96.715				
30	.246	.702	97.418				
31	.228	.653	98.070				
32	.199	.568	98.638				
33	.177	.506	99.144				
34	.164	.468	99.613				
35	.136	.387	100.000				

Extraction Method: Principal Component Analysis.

Figure 3 Harman's single-factor test

3.11 Ethical Consideration

Any research plan must take ethics into account, especially when using human participants. The importance of upholding the highest ethical standards throughout the research process is emphasized by the researcher in this study. The secrecy of the respondents' information is one of the main ethical issues that the proposal addresses. Participants are reassured by the researcher that their answers will be kept private and used only for study. The study underlines the importance of informed consent. Participants will get clear explanations of the study's goals and the nature of their involvement without suffering any consequences. To ensure that participants are aware of the full extent of their involvement and can make an informed decision about their participation in the study, this transparency is essential. By obtaining informed consent, the researcher upholds ethical research practices and respects the participants' autonomy.

Research Time Schedule and Budget

	Month							
Activity	**Oct**	**Nov**	**Dec**	**Jan**	**Feb**	**Mar**	**Apr**	**May**
Searching for titles by reviewing different literatures	**X**							
Deciding the title and start working on the proposal		**X**	**X**					
Finalyzing and submitting the proposal			**X**					
Distributing and collecting data				**X**	**X**			
Analyzing the data						**X**		
Finalizing the document						**X**	**X**	
Submit the paper and presentation preparation								**X**

Table 4 Time Schedule

Items	**Quantity**	**Unit cost in Birr**	**Total cost in Birr**
Secretarial Services			
i) Secretarial	80 Pages	8	640
ii) Photocopy and print	80 Pages	5	400
Stationery requirement			
i) Flash Disc	1	400	400
ii) paper	2	400	800
iii) Pen	2	35	70
Transportation			1000
Other expenses			1000
Total			**4310**

Table 5 Budget

Chapter Four

DATA Presentation, Analysis and Discussion

4.1 Introduction

This Chapter mainly contains the analysis, interpretation and presentation of the data and responses gathered from the questionnaires as a primary source. The information's and responses are presented using basic descriptive, correlation, regression and mediation analyses. The data presented using different tables and each expressed verbally.

4.2 Response Rate

To collect information's from respondents a questionnaire was implied. From total distributed 206 questionnaires 186 were responded with 90.29 % response rate. SPSS is used to analyze all the collected data.

4.3 Demographic Characteristics

Table 6 Demographic Characterstics

No.	Description		Respondent		Total	
			Frequency	%	N	%
1	Gender	M	103	55.4	186	100
		F	83	44.6		
2	Age	Below 25	15	8.1	186	100
		25-34	85	45.7		
		35-44	62	33.3		
		45-54	23	12.4		
		55 and above	1	0.5		
3	Education Level	High School	15	8	186	100
		Bachelors Degree	116	62.4		
		Masters Degree	55	29.6		
		PHD	0	0		
4	Years of experience at Ethswitch	<1	12	6.5	186	100
		1-3 years	34	18.3		
		4-5 years	44	23.7		
		6-8 years	56	30.1		
		>9	40	21		
5	Job Role	CIO(Chief Information Officer)	60	32.2	186	100

		COO(Chief Operation Officer)	58	31.2		
		CCO(Chief Corporate Officer)	45	24.2		
		CPO(Chief Portfolio Officer)	23	12.4		

Source: Self Survey (2026)

There are more male respondents than female while comparing the gender distribution of respondents. From total 186 respondents 103 were males which is accounted about 55.4 % and 83 were females which is 44.6 percent of the respondents.

The age distribution of the respondents that responded the questionnaire holds mostly young individuals. The biggest concentrated group is aged between 25-34 years with 85 people (45.7 %) in this range. The next age group is 35-44 years, which includes 62 people (33.3 %). The group aged 45-54 has holds 23 people (12.4 %). A smaller number, 15 participants (8%), are belongs to younger than 25 years. Those aged 55 and up represent the smallest group, with just 1 person (0.5 %). This pattern really highlights the youth dominance in the sample data.

The education level of respondents is mainly at the Bachelor's degree level or holds BSC and BA degrees, with 116 people (62.4 %). The next groups are those holding a Master's degree, making up 55 people (29.6 %). A small group of 15 people (8%) have just a high school education. There is 0 number of PHD holder from the respondents.

The experience level of the respondents ranged from 6-8 years is the highest number from the respondents which is 56 respondents (30.1%). The following experience group is ranged from 4-5 years with 44 respondents which is 23.7 %. The next experience level is >9 years with 40 respondents (21%). Experience level ranged from 1-3 holds 34 respondents that is 18.3 %. Experience level with <1 is the least number with 12 respondents accounted for 6.5 %.

The respondents come from diverse educational backgrounds and have notable representation from number of different important teams and departments. The CIO team holds the largest group with 60 respondents which is accounted about (32.2%). The COO team follows the CIO team closely with 58 respondents accounted for

(31.2%). The CCO team shows 45 respondents having (24.2%) and the CPO team includes the smallest respondents which is 23 respondents (12.4%).

4.4 Reliability Results and Validity Analysis

4.4.1 Reliability Result

Table 7 Reliablity Result

Variables	No. of Items	Cronbach Alpha	Interpretation
Attitude	5	0.813	Good
Subjective Norm	5	0.808	Good
Perceived Behavioural Control	5	0.793	Acceptable
Intention	5	0.912	Excellent
Habit	5	0.835	Good
Regret	5	0.824	Good
Compliance Behaviour	5	0.924	Excellent

Source: Self Survey (2026)

The Cronbach Alpha reliability results shows that all the constructs or variables on the survey are at least meeting the minimum acceptable range of reliability which is >0.7. From Excellent to acceptable results are shown in the study which shows a very good internal consistency. All of the seven constructs or variables shows a level of internal consistency, with the Cronbach Alpha ranging from 0.793 to 0.924. The highest levels of reliability were observed for the Information Security Policy Compliance Behavior ($\alpha = 0.924$), Intention ($\alpha = 0.912$) constructs, all indicating excellent levels of reliability. The results also showed the Habit ($\alpha = 0.835$), Regret ($\alpha = 0.824$), Attitude ($\alpha = 0.813$) and Subjective Norm ($\alpha = 0.824$) constructs possessing good reliability. The only construct that shows lower scale with acceptable range is Perceived Behavioral control ($\alpha = 0.793$). Although each scale only consists of five items, the alpha values are nonetheless sound, particularly as the items are all working well within each construct to measure the theoretical concept. The reliability of the scales therefore suggests that they are adequate for use in the current study to measure the variables in appropriate relationships since they are internally consistent.

4.4.2 Validity Analysis

Validity testing was performed to determine if the questionnaire items in this study effectively measured the targeted constructs. Both construct validity and convergent/discriminant validity were evaluated through exploratory factor analysis and correlation-based methods. The procedures involved the Kaiser-Meyer-Olkin

(KMO) measure, Bartlett's Test of Sphericity, Exploratory Factor Analysis (EFA), and correlation-based evaluations of convergent and discriminant validity.

4.4.2.1 Kaiser-Meyer-Olkin (KMO) and Bartlett's Test

Before performing exploratory factor analysis (EFA), the dataset's adequacy and the data's suitability for factor analysis were assessed using the Kaiser-Meyer-Olkin (KMO) measure and Bartlett's Test of Sphericity. The KMO statistic assesses sampling adequacy, while Bartlett's test determines if the variables are sufficiently correlated.

Table 8 KMO and Bartlett

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.926
Bartlett's Test of Sphericity	Approx. Chi-Square	3598.099
	df	595
	Sig.	.000

The KMO value for the behavioural items (R1-R11) was 0.926, which is considered "excellent" according to Kaiser's (1974) classification. A value above 0.90 suggests that the correlations between variables are strong enough to proceed with factor analysis and that the sample size is sufficient.

Additionally, Bartlett's Test of Sphericity showed a highly significant result (χ^2 = 3598.099, df = 595, $p < 0.000$), indicating that the correlation matrix is not an identity matrix, and the items are sufficiently intercorrelated to justify factor extraction. These results confirm that the dataset meets the basic assumptions for conducting EFA to examine the construct structure of the behavioural item scales.

4.4.2.1 Exploratory Factor Analysis (EFA)

An exploratory factor analysis utilizing principal component analysis with Promax rotation was performed in order to determine the underlying structure of the information security compliance items. Seven components with eigenvalues greater than 1 were identified consistent with the hypothesized theoretical model. The first component was

made up of items about habitual compliance behavior (HAB1-HAB5), which represented an automatic and enacted mode of compliance to information security policy. The second component had items of intention (Int1-Int5) which, as would be expected, determined intention to comply with the information security policy. The third component was attitude (Att1-Att5) accounting for positive evaluations of having complied with the information security policy, and the fourth was perceived behavioral control (PBC1-PBC5), about people's confidence that they would be able to comply. The 5th component consisted of the Regret items (Reg1–Reg5), which represented how much pressure participants viewed they were under to obey from their superiors, coworkers, and the organization. The 6th component consisted of the Subjective scale items (SN1–SN5), which represented people's evaluation of what their compliance decisions in the past. The 7th component represented compliance behaviour (Act1–Act5) self-reports. In general, the loadings were good with all items loading significantly above the minimum standard of 0.50 on their respective components. Most items loaded clearly onto their defined constructs and the structure agreed with the theory. This indicates a strong measurement model.

Table 9 EFA

Item	C1	C2	C3	C4	C5	C6	C7
HAB1	0.837						
HAB2	0.665						
HAB3	0.707						
HAB4	0.76						
HAB5	0.591						
Int1		0.803					
Int2		0.84					
Int3		0.796					
Int4		0.646					
Int5		0.709					
Att1			0.699				
Att2			0.736				
Att3			0.68				
Att4			0.826				
Att5			0.677				
PBC1				0.581			
PBC2				0.636			
PBC3				0.621			
PBC4				0.580			
PBC5				0.84			
Reg1					0.872		

Reg2					0.545		
Reg3					0.816		
Reg4					0.748		
Reg5					0.672		
SN1						0.729	
SN2						0.752	
SN3						0.711	
SN4						0.681	
SN5						0.737	
ISP_Beh1							0.578
ISP_Beh2							0.628
ISP_Beh3							0.651
ISP_Beh4							0.666
ISP_Beh5							0.742

4.4.2.1 Convergent and Discriminant Validity

Pearson correlations between the Study Variables were used to determine the construct validity of the constructs. Convergent validity was observed as the intended constructs had statistically significant, moderately high to high positive correlations. For example, intention had high correlations with attitude (r = .611), perceived behavioral control (r = .649) and compliance behaviour (r =.672).

Discriminant validity was achieved by ensuring that the inter-construct correlations did not exceed the common guidelines of 0.85. With the inter-construct correlations ranging from 0.358 to 0.687, this implies that each construct was indeed measuring a unique set of information security compliance behavior.

So, we can conclude that internal convergence and discriminant distinctiveness validity is evident from the correlation matrix.

Table 10 Convergent and Discriminant

Construct	Attitude	SN	PBC	Reg	Habit	Intention	ISP Behavior
Attitude	1	.421**	.398**	.376**	.369**	.611**	.511**
SN	.421**	1	.482**	.391**	.358**	.597**	.425**
PBC	.398**	.482**	1	.404**	.421**	.649**	.673**
Reg	.376**	.391**	.404**	1	.532**	.477**	.509**
Habit	.369**	.358**	.421**	.532**	1	.466**	.687**

Intention	.611**	.597**	.649**	.477**	.466**	1	.672**
ISP Behavior	.511**	.425**	.673**	.509**	.687**	.672**	1

4.5 Descriptive Statistics

For the data collected from the questionnaire the researcher used descriptive analysis to describe the variables in different aspects. Mean and Standard deviation is presented in this analysis of the respondent. Following are the study presented the result of the mean and standard deviation of each construct.

4.5.1 Descriptive Analysis of Attitude

Table 11 Attitude Descriptive Statistics

Descriptive Statistics

	N	Mean	Std. Deviation
I feel that compliance with the Information Security Policy (ISP) is a positive thing.	186	3.84	.715
I feel that compliance with the ISP is reasonable.	186	3.80	.688
I feel that compliance with the ISP is important.	186	3.83	.606
Following the Information Security Policy is a good idea.	186	3.80	.587
Following the Information Security Policy is pleasant.	186	3.82	.678
Valid N (listwise)	186		

Source: Self Survey (2026)

The five items related to attitude shows close descriptive statistics result comparing with each other. The mean scores are in between 3.80 and 3.84 and all the standard deviations are measured below 0.715 which shows the responses are not varied that much from respondents to respondent. The highest mean is related with the statement "I feel that compliance with the ISP is a positive thing" with (Mean = 3.84, SD = 0.715). The two statements with the lowest mean "I feel compliance is reasonable" and "Following the ISP is a good idea" shows identical or same results with their Mean at 3.80 and they have a variance of 0.688 and 0.589 respectively. All items received scores

above 3.80 according to this study. The results show that respondents hold a positive attitude about information security policy compliance. According to the study most employees have the same perception about information compliance behaviour, also they share the same and steady acceptance on compliance. So, the uniform moderate positive attitude shows that rather than strong personal motivation or perception, employees follow security policies as part of their job. This benefits the company since compliance is accepted.

The standard deviations for the individual items range from 0.587 to 0.715, with an overall average standard deviation about 0.65. The participants answered the questions with high consistency because they showed low response variability among the responses and there is a limited diversity about on their perception to information security policies. So, this shows there is small or little disagreement on security compliance, indicating that the employees mostly understand and apply the policies in a uniform and similar way. So for the improvement and strong motivation actions should be taken in over all the company instead of focusing some specific group.

4.5.2 Descriptive Analysis of Subjective Norm

Table 12 Subjective Norm Descriptive Statistics

Descriptive Statistics

	N	Mean	Std. Deviation
Top management believes I should comply with the organization's information security policies.	186	3.91	.655
My boss believes I should comply with the organization's information security policies.	186	3.83	.712
My colleagues believe I should comply with the organization's information security policies.	186	3.85	.686
The information security department in my organization believes I should comply with information security policies.	186	3.88	.647
Other technical computer specialists in the organization believe I should comply with information security policies.	186	3.80	.704
Valid N (listwise)	186		

Source: Self Survey (2026)

The items related to Subjective Norm shows nearly varied descriptive statistics result comparing with each other. The mean scores are in between 3.80 and 3.91 and all the

standard deviations are measured below 0.712 which shows the responses are not varied that much from one respondent to another respondent. The highest mean is associated with the statement " Top management believes I should comply with the organization's information security policies." with (Mean = 3.91, SD = 0.655). The statement with the least Mean (Mean = 3.80, SD = 0.704) is " Other technical computer specialists in the organization believe I should comply with information security policies.". All items received scores above 3.80 according to this study. The results show that respondents feel their colleague, management and peer pressure on complying with information security policy. That social pressure is probably effective. For the organization it establishes a positive compliance, where behaviour is partially determined by the perceptions of what other people think the individual should do, rather than his or her own perceptions alone. But, given that the scores are still only mildly high, this effect alone may not be sufficient to produce full compliance. Reinforcing perceived expectations with more visible manager behaviour and peer pressure may benefit the company. The standard deviations for the individual items range from 0.647 to 0.712, with an overall average standard deviation about 0.68. pressure exists irrespective of the group and it may actually be more reassuring that there seems the social pressure have less variation. Therefore, in order to sustain compliance behaviour, it might be necessary for the organization to continue address each department with reinforcing messages.

4.5.3 Descriptive Analysis of Perceived Behavioural Control

Table 13 Pereceived Behavioural Control Descriptive Statistics

Descriptive Statistics

	N	Mean	Std. Deviation
I have the necessary skills to comply with the organization's Information Security Policy (ISP).	186	3.76	.656
I have the expertise to implement preventive measures, in line with the ISP, to protect my confidential information and organizational computers from harm.	186	3.76	.648
I believe it is within my control to comply with the Information Security Policy (ISP).	186	3.85	.670
For me, following the security procedures described in the Information Security Policy (ISP) is easy.	186	3.80	.664

My ability to comply with the Information Security Policy (ISP) and prevent security violations is adequate.	186	3.85	.704
Valid N (listwise)	186		

Source: Self Survey (2026)

The five items related to Perceived Behavioral Control shows nearly varied descriptive statistics result comparing with each other. The mean scores are in between 3.76 and 3.85 and all the standard deviations are measured below 0.704 which shows the responses are not varied that much from one respondent to another respondent while compared each other. The highest Mean's are related with the statement " My ability to comply with the Information Security Policy (ISP) and prevent security violations is adequate." and " I believe it is within my control to comply with the Information Security Policy (ISP)." with (Mean = 3.85, SD = 0.704) and (Mean = 3.85, SD = 0.670) respectively. The two other statements with the least mean " I have the necessary skills to comply with the organization's Information Security Policy (ISP)." and " I have the expertise to implement preventive measures, in line with the ISP, to protect my confidential information and organizational computers from harm." both have their average scores at (Mean = 3.76, SD = 0.656) and (Mean = 3.76, SD = 0.648) respectively. All items received scores above 3.76 according to this study. The results show that respondents feel they are capable and they are in control on following or complying with information security policy. This is important for the company because it indicates compliance is not perceived as technically daunting or complex. Think of it like this: when individuals perceive themselves as capable and in control, it is much more likely the individual will actually demonstrate compliance in the long run, even when their motivation to perform that behaviour differs. However, as the scores lie in the middle rather than the very high range, it is probable that some employees will only perceive themselves as "reasonably" empowered, so ongoing training and practical assistance may still help to enhance actual compliance. The standard deviations for the individual items range from 0.648 to 0.704, with an overall average standard deviation of about 0.67. The values show that participants answered the questions with low response variability among the responses. This is beneficial for the company as it indicates that the employees are relatively in agreement about how capable they believe themselves to be to achieve ISP dependability, and therefore the likelihood of low skills or confidence-in-ability resulting in variable compliance is minimized.

4.5.4 Descriptive Analysis of Habit

Table 14 Habit Descriptive Statistics

Descriptive Statistics

	N	Mean	Std. Deviation
Complying with information security policies is something I do frequently.	186	3.91	.676
Complying with information security policies is something I do automatically.	186	3.86	.729
Complying with information security policies is something I do without having to consciously remember to do so.	186	3.85	.678
Complying with information security policies is something that belongs to my routine.	186	3.93	.658
Complying with information security policies is something I would find hard not to do.	186	3.89	.668
Valid N (listwise)	186		

Source: Self Survey (2026)

The listed items related to Habit shows nearly varied descriptive statistics result comparing with each other. The mean scores are in between 3.85 and 3.93 and all the standard deviations are measured below 0.729 which shows the responses are not varied that much from one respondent to another respondent. The highest mean is associated with the statement "Complying with information security policies is something that belongs to my routine." with (Mean = 3.93, SD = 0.658). The next statement " Complying with information security policies is something I do frequently." Shows (Mean = 3.91, SD = 0.676). The subsequent statement " Complying with information security policies is something I would find hard not to do." shows (Mean = 3.89, SD = 0.668). The statement " Complying with information security policies is something I do automatically." Has (Mean = 3.86, SD = 0.729). The statement with the least Mean (Mean = 3.85, SD = 0.678) is " Complying with information security policies is something I do without having to consciously remember to do so.". All items received scores above 3.85 according to this study. The results show that respondents developed strong habit on following or complying security policies and it becomes part of their daily routine or they are doing it regularly. This is great for the company as it shows a

growing independence from both pressure and reminders. It has a strong potential for self-sustainability once a certain threshold of compliance is reached. However, where compliance is almost perfect, the reinforcement is likely to slowly decay. Interestingly, the strong scores combined with a presumed positive sign, would imply that a looped system of reminders would create effortless and pleasant habits over time. The standard deviations for the individual items range from 0.658 to 0.729, with an overall average standard deviation about 0.68. The values show that participants answered the questions with high consistency. For the company, that consistency is a good sign because it means compliance isn't isolated to certain groups it's becoming a general working pattern.

4.5.5 Descriptive Analysis of Regret

Table 15 Regret Descriptive Statistics

Descriptive Statistics

	N	Mean	Std. Deviation
Following the information security policy was the right decision.	186	3.77	.626
I didn't regret the way I complied to the information security policy.	186	3.80	.625
I would follow the same compliance decision regarding the information security policy again.	186	3.84	.668
My decision regarding the information security policy caused positive consequences.	186	3.80	.680
My decision regarding the information security policy was wise.	186	3.84	.710
Valid N (listwise)	186		

Source: Self Survey (2026)

Regret shows nearly varied descriptive statistics result comparing with each other. The mean scores are in between 3.77 and 3.84 and all the standard deviations are measured below 0.710 which shows the responses are not varied that much from one respondent to another respondent while compared each other. The highest Mean's are related with the statement " I would follow the same compliance decision regarding the information security policy again." and " My decision regarding the information security policy was wise." with (Mean = 3.84, SD = 0.668) and (Mean = 3.84, SD = 0.710) respectively. The statement with least Mean is "Following the information security policy was the

right decision." with (Mean = 3.77, SD = 0.626). All items received scores above 3.77 according to this study. The results show that the respondents are generally feels good about their past experiences on complying with the information security policy. From the company's perspective, this is positive because it means there is decreased cognitive assumption following their compliance and they are less likely to change their behavior in negative ways in the future. Even if it is moderately positive it shows that this positive reflection is present but not deeply strong or emotionally driven. The standard deviations for the individual items range from 0.625 to 0.710, with an overall average standard deviation of about 0.66. The values indicate a consistency in responses among the employees. This consistency is useful to the company because it means that, for the most part, employees are aligned in their perceptions of their choices. While not overly enthusiastic, these predominantly positive sentiments suggest that focusing on reinforcing these feelings could help strengthen future compliance.

4.5.6 Descriptive Analysis of Intention

Table 16 Intention Descriptive Statistics

Descriptive Statistics

	N	Mean	Std. Deviation
I am likely to comply with my organization's information security policies.	186	4.24	.598
It is possible that I will follow information security policies to help protect the organization's information systems.	186	4.23	.562
I am certain that I will act in accordance with the organization's information security policies.	186	4.21	.592
I intend to comply with the requirements of my organization's Information Security Policy (ISP) in the future.	186	4.26	.570
I intend to safeguard information and technology resources and carry out my assigned responsibilities as outlined in the ISP when using organizational information and technology.	186	4.26	.596
Valid N (listwise)	186		

Source: Self Survey (2026)

Intention items show close descriptive statistics result comparing with each other. The mean scores are in between 4.21 and 4.26 and all the standard deviations are measured below 0.598 which shows the responses are not varied that much from respondents to respondent. The highest Mean's are related with the statement " I intend to comply with the requirements of my organization's Information Security Policy (ISP) in the future." and " I intend to safeguard information and technology resources and carry out my assigned responsibilities as outlined in the ISP when using organizational information and technology." with (Mean = 4.26, SD = 0.570) and (Mean = 4.26, SD = 0.596) respectively. The statement with least Mean is " I am certain that I will act in accordance with the organization's information security policies." with (Mean = 4.21, SD = 0.592). All items received scores above 4.21 according to this study. The results show that respondents are highly intended to comply with information security policy. That is a significant result for the organization because intentions are usually the nearest proximity before behaviours. This policy has already been absorbed by employees instead of just following as a theory. They intend to comply with it, especially as it relates to the protection of critical infrastructure and fulfilling the responsibilities of their role. While there is some variation from item to item, the data suggests employees are generally intent on complying with this policy, and are not strongly influenced by particular details. The standard deviations for the individual items range from 0.562 to 0.598, with an overall average standard deviation about 0.58. For the organization it is a good consideration as it shows consistent behavioural direction with no disagreement between employees. Therefore the challenge for the organization now will be how to turn the intention strength into compliance behavior in day to day contexts since employees shared intention similarly.

4.5.7 Descriptive Analysis of ISPC Behaviour

Table 17 ISPC Behaviour Descriptive Statistics

Descriptive Statistics

	N	Mean	Std. Deviation
I comply with the Information Security Policy (ISP).	186	3.80	.589
I recommend that others comply with the Information Security Policy (ISP).	186	3.85	.623

I assist others in complying with the Information Security Policy (ISP).	186	3.85	.596
I follow the security procedures described in the Information Security Policy (ISP).	186	3.83	.600
I apply the requirements of the Information Security Policy (ISP) when using organizational information and technology.	186	3.89	.597
Valid N (listwise)	186		

Source: Self Survey (2026)

ISPC Behaviour shows close descriptive statistics result comparing with each other. The mean scores are in between 3.80 and 3.89 and all the standard deviations are measured below 0.623 which shows the responses are not varied that much from respondents to respondent. The highest mean is related with the statement " I apply the requirements of the Information Security Policy (ISP) when using organizational information and technology." with (Mean = 3.89, SD = 0.597). The statement with least Mean is " I comply with the Information Security Policy (ISP)." with (Mean = 3.80, SD = 0.589). All items received scores above 3.75 according to this study. The results show that respondents show a good level of ISP compliance. The company establishes a base level of trust because its actual practices demonstrate compliance which exists beyond mere employee attitudes and their intended behaviors. The standard deviations for the individual items range from 0.589 to 0.623, with an overall average standard deviation about 0.60. The organization gains valuable benefits from its consistent operations because its compliance duties remain consistent throughout all staff members instead of showing uneven implementation. When an organization shows such strong behavioral patterns because of its ongoing requirements for compliance training, it means that all employees need more time to develop their actual compliance abilities which should reach a level of complete proficiency.

4.6 Inferential Analysis

4.6.1 Correlation Analysis

Table 18 Correlation Analysis

Correlations

	Attitude	SN	PBC	Reg	Hab	Int	ISP_Beh

Attitude	Pearson Correlation	1	.421**	.398**	.376**	.369**	.611**	.511**
	Sig. (2-tailed)		.000	.000	.000	.000	.000	.000
	N	186	186	186	186	186	186	186
SN	Pearson Correlation	.421**	1	.482**	.391**	.358**	.597**	.425**
	Sig. (2-tailed)	.000		.000	.000	.000	.000	.000
	N	186	186	186	186	186	186	186
PBC	Pearson Correlation	.398**	.482**	1	.404**	.421**	.649**	.673**
	Sig. (2-tailed)	.000	.000		.000	.000	.000	.000
	N	186	186	186	186	186	186	186
Reg	Pearson Correlation	.376**	.391**	.404**	1	.532**	.477**	.509**
	Sig. (2-tailed)	.000	.000	.000		.000	.000	.000
	N	186	186	186	186	186	186	186
Hab	Pearson Correlation	.369**	.358**	.421**	.532**	1	.466**	.687**
	Sig. (2-tailed)	.000	.000	.000	.000		.000	.000
	N	186	186	186	186	186	186	186
Int	Pearson Correlation	.611**	.597**	.649**	.477**	.466**	1	.672**
	Sig. (2-tailed)	.000	.000	.000	.000	.000		.000
	N	186	186	186	186	186	186	186
ISP_Beh	Pearson Correlation	.511**	.425**	.673**	.509**	.687**	.672**	1
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	
	N	186	186	186	186	186	186	186

**. Correlation is significant at the 0.01 level (2-tailed).

Source: Self Survey (2026)

Regarding the information Security Policy compliance several kinds of relationships are shown between the variables used in the study. The highest positive relationship is seen between Perceived behavioral control and Information security compliance behavior which is ($r=0.673$, $p<0.1$). This implies that Whenever employees feel that they are capable of following the security policy they are more likely just do that and comply with it. Habit also shows a similar high relation with ISPC behaviour which is

(r = .687, p < .01), that shows once compliance becomes a routine or habitual action most likely it will have a continues repetition.

Intention is also one of the variables that has a strong relationship with ISPC behavior with (r = .672, p < .01), showing that people with clearer intention to comply with Information security most likely to act on it or doing it. Information security policy compliance behaviour also has a moderate relationship with Attitude (r = .511, p < .01), that clearly express positive attitude towards a compliance behaviour really matters. Regret and Subjective norm also has a moderate relationship with ISPC behaviour that shows past experience, feelings and peer, colleague, management influences has a role on comping with information security policy.

Perceived Behavioral Control also has a strong relationship with Intention (r = .649, p < .01), showing people that feel capable of complying will be intended to comply. Attitude (r = .611, p < .01) and Subjective Norm (r = .597, p < .01) also have a strong relationship with intention. This suggests intention is affected by how people think, how much control they feel they possess, and the expectations of those around them. although the connections aren't as strong, Habit (r = .466, p < .01) and Regret (r = .477, p < .01) also relate to intention.

Most relationships among the independent variables themselves are moderate. For instance, Regret and Habit are reasonably related (r = .532, p < .01), and Subjective Norm and Perceived Behavioural Control also shows a notable relation which is (r = .482, p < .01). These findings imply that while the variables are interrelated, they don't overlap excessively with each other. Overall, the pattern is pretty consistent, even if several factors are important, Perceived Behavioural Control, Habit, and Intention are more prominent in relation to actual compliance behaviour.

4.6.2 Assumption of Multiple Linear Regression

4.6.2.1 Intention (Model 1)

Multicollinearity Test

Table 19 Model 1 Multicollinearity Test

Model		Collinearity Statistics	
1		Tolerance	VIF
	(Constant)		

	Att	0.729	1.371
	Subj	0.677	1.476
	Perc	0.663	1.509
	Hab	0.648	1.543
	Reg	0.644	1.553
a. Dependent Variable: Int			

Source: Self Survey (2026)

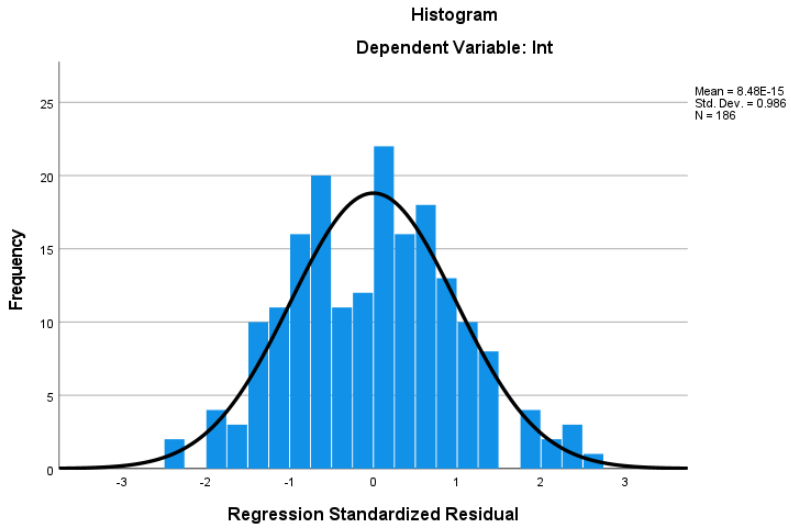
In order to make sure the independent variables were not interrelated to each other a multicollinearity test was conducted as it should be done prior to proceeding with the regression analysis as it could impair the reliability of the results. Variance Inflation Factor (VIF) and Tolerance Value was used to appraise.

When observing the results, all predictors Attitude, Subjective Norm, Perceived Behavioural Control, Habit and Regret have VIF range from 1.371 to 1.553, which are significantly below usually accepted threshold of 5. Concurrently, their Tolerance Values ranges from 0.644 and 0.729, clearly more than the lowest acceptable level of 0.1.

These values shows that multicollinearity is not the concern in this model. This means that the independent variables Attitude, Subjective Norm, Perceived Behavioural Control, Habit, and Regret are not excessively or highly overlapping with each other. All of the mentioned independent variables have a contribution in explaining intention that will allow proceeding the regression analysis with out a concern on multicollinearity issue.

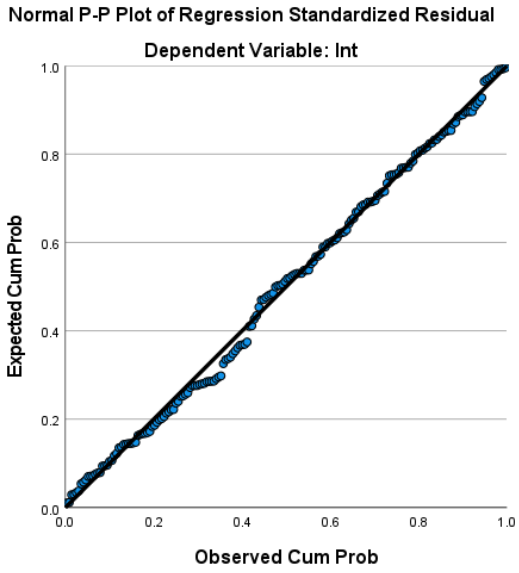
Normality Test

Figure 4 Model 1: Histogram



Source: Self Survey (2026)

Figure 5 Model 1: P-P Plot



Source: Self Survey (2026)

A normality assumption was checked to identify whether the residuals are approximately normally distributed before regression analysis. We should check normality assumption, because the regression analysis basically relies on normality errors. If these residuals show a normal distribution, then the regression analysis will be reliable and unbiased. To asses the data both histogram and P-P plot were checked.

The histogram diagram shows a reasonable symmetric distribution and it has a bell shape pattern. The values are mostly concentrated in the centre, with some values shows at the end of the curves which is as expected in the normal condition. The ends of both

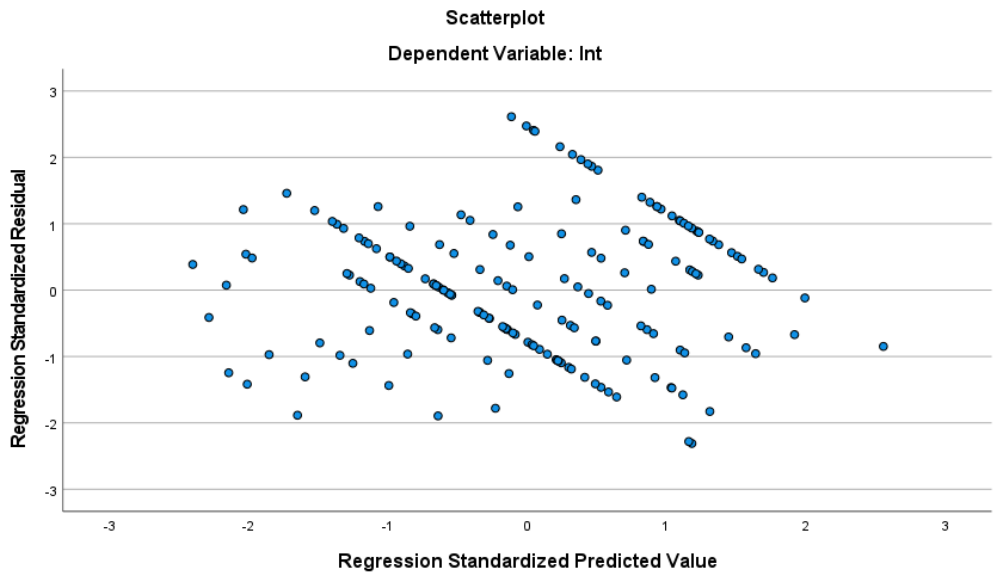
tails appear a little non-normal, but nothing sufficient to violate the assumption of normality. It's not uncommon for these slight variations to show up.

The regular P-P plot adds further proof to the earlier statement. The plotted points are nearby the diagonal line, which is the reference line. Consequently, if the values were normal, the observed cumulative probabilities are close to the expected cumulative probabilities. Some parts of the plot do show points that fall a little away from the diagonal line. However, these do not constitute serious violations of normality.

Checking together Histogram and P-P plot shows that there is an approximate normal distribution of the residuals. So, from the findings we can confirm that the assumption of normality is satisfied and the regression analysis can procced.

Linearity Test

Figure 6 Model 1: Scatterplot



Source: Self Survey (2026)

Scatterplot of standardized residuals was tested against the standard predicted variables for the linearity assumption. There is no clear curved or strong pattern like a wave or U-shaped is not shown in the plot instead the points show randomly scattered manner across the plots. This suggests a linear relationship between the dependent and independent variables. So, the above plot suggests that the model is suitable for further regression analysis.

Homoscedasticity Test

The assumption that the residuals variance being constant around the predicted value is called Homoscedasticity, and violation of these assumptions can result in inefficiency and unreliable estimates of the regression. This homoscedasticity was checked using standardized residuals plot against the standardized predicted values, as shown in the above scatterplot diagram the points are dispersed generally in a random pattern with no identifiable systematic pattern or funnel shape. So, the approximate constant variance of the residuals implies that the homoscedasticity assumption is satisfied and further regression analysis can continue with regression analysis.

4.6.2.2 Information Security Policy Compliance Behaviour (Model 2)

Multicollinearity Test

Table 20 Model 2 Multicollinearity Test

Model		Collinearity Statistics	
		Tolerance	VIF
1	(Constant)		
	Perc	0.578	1.729
	Int	0.578	1.729
a. Dependent Variable: ISP_Beh			

Source: Self Survey (2026)

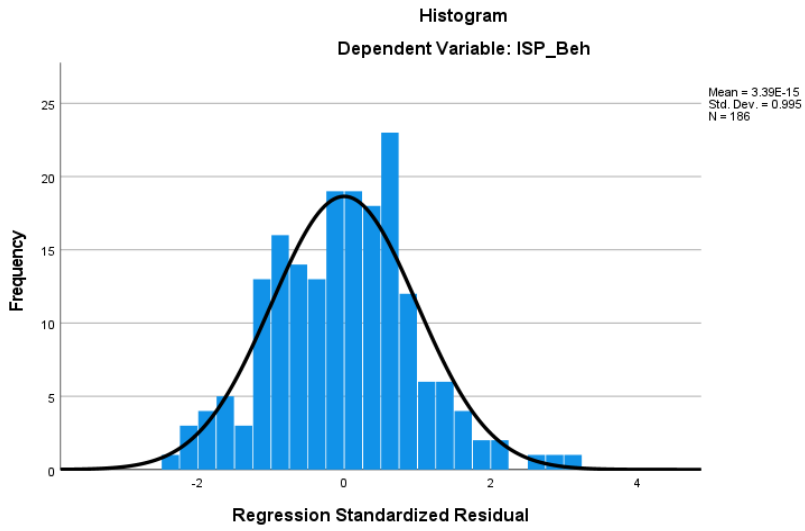
In order to make sure the independent variables were not interrelated to each other a multicollinearity test was conducted as it should be done prior to proceeding with the regression analysis as it could impair the reliability of the results. Variance Inflation Factor (VIF) and Tolerance Value was used to appraise.

When observing the results, both predictors Perceived Behavioural Control (PBC) and Intention have the same VIF values 1.729, which are significantly below usually accepted threshold of 5. Concurrently, their Tolerance values are 0.578, which is clearly more than the lowest acceptable level of 0.1.

The above values shows that multicollinearity is not the concern in this model. Even if Perceived Behavioural Control (PBC) and Intention are linked, they are not related to an extent of affecting the regression results, So the next regression analysis can be confirmed to continue since each variable provide a significant and unique information in briefing ISP compliance behaviour.

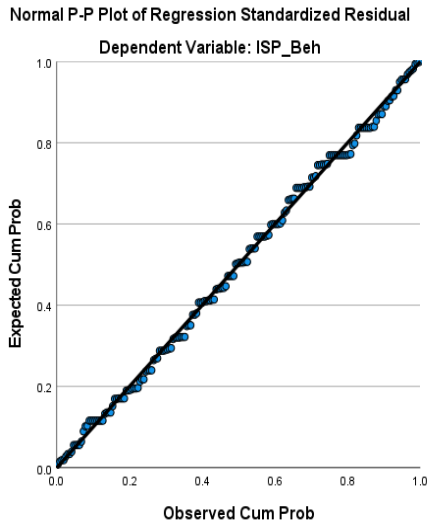
Normality Test

Figure 7 Model 2: Histogram



Source: Self Survey (2026)

Figure 8 Model 2: P-P Plot



Source: Self Survey (2026)

A normality assumption was checked to identify whether the residuals are approximately normally distributed before regression analysis. Also, we should check normality assumption, because the regression analysis basically relies on normality errors, if these residuals show a normal distribution, then the regression analysis will be reliable. To assess the data both histogram and P-P plot were checked.

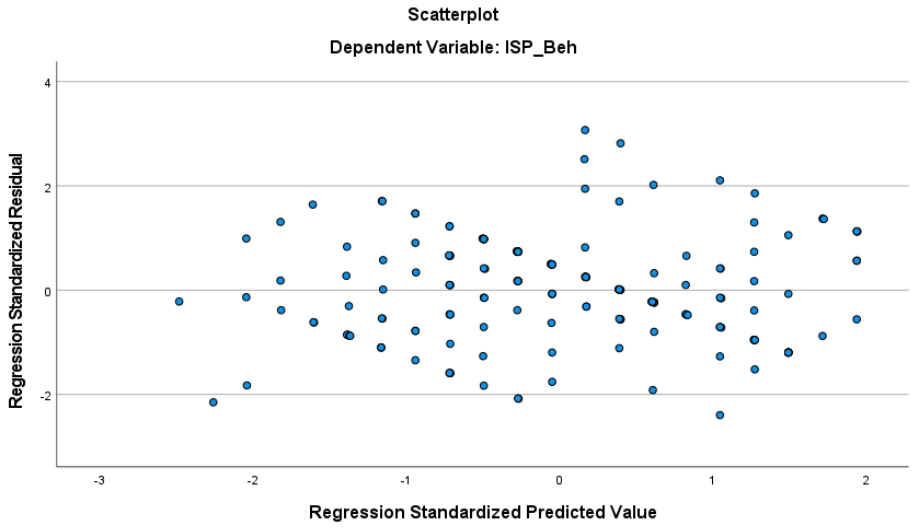
The histogram diagram shows a reasonable symmetric distribution and it has a bell shape pattern and most of the values are concentrated in the center, with some values shows at the end of the curves which is as expected in the normal condition.

While checking the P-P plot diagram the plotted points are nearby the diagonal line, which is the reference line. Consequently, if the values were normal, the observed cumulative probabilities are close to the expected cumulative probabilities.

Checking together Histogram and P-P plot shows that there is an approximate normal distribution of the residuals so, we can conclude from the findings that the assumption of normality is satisfied and the regression analysis can procced.

Linearity Test

Figure 9 Model 2: Scatterplot



Source: Self Survey (2026)

Scatterplot of standardized residuals was tested against the standard predicted variables for the linearity assumption. There is no clear curved or strong pattern like a wave or U-shaped is not shown in the plot instead the points show randomly scattered manner across the plots. This suggests a linear relationship between the dependent and independent variables. So, the above plot suggests that the model is suitable for further regression analysis.

Homoscedasticity Test

The assumption that the residuals variance being constant around the predicted value is called Homoscedasticity, and violation of these assumptions can result in inefficiency

and unreliable estimates of the regression. This homoscedasticity was checked using standardized residuals plot against the standardized predicted values, as shown in the above scatterplot diagram the points are dispersed generally in a random pattern with no identifiable systematic pattern or funnel shape. So, the approximate constant variance of the residuals implies that the homoscedasticity assumption is satisfied and further regression analysis can continue with regression analysis.

4.6.3 Multiple Linear Regression

The multiple linear regression model was used to examine the influence of five independent variables Attitude, Subjective Norm, Perceived Behavioural control, Habit, and Regret on the dependent variable, Information Security Policy compliance through mediating effect of intention.

4.6.3.1 Intention (Model 1)

4.6.3.1.1 Model Summary

Table 21 Model 1: Model Summary

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig.F Change
1	.796[a]	.633	.623	.30825	.633	62.143	5	180	<.001

a. Predictors: (Constant), Hab, SN, Attitude, PBC, Reg

b. Dependent Variable: Int

Source: Self Survey (2026)

The above regression model shows that intention is highly explained by the predictor variables (Attitude, Subjective Norm, Perceived Behavioral Control, Habit and Regret) since the R^2 value is 0.633. This indicates that 63.3 % of the variance in intention is explained by the above mentioned variables. Also, the model is significant (F = 62.143, p = <.001), which shows that the predictors collectively give a meaningful result as opposed to the result happening by chance and the general relationship also has a very strong value, as shown in the R value of 0.796. The model is stable and not overfit as

the value of adjusted R^2 (0.623) is very close to the R^2, and the relative standard error which is 0.30825 tells that the predictions are fairly accurate. The above findings indicate that these behavioral variables have a significant and impact on the intention of the employees toward adhering to information security policies.

4.6.3.1.2 ANOVA Test

Table 22 Model 1: ANOVA Test

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	29.523	5	5.905	62.143	<.001[b]
	Residual	17.103	180	.095		
	Total	46.626	185			

a. Dependent Variable: Int

b. Predictors: (Constant), Hab, SN, Attitude, PBC, Reg

Source: Self Survey (2026)

The general significance of the regression model on explaining Intention is shown by the ANOVA results. The F value (62.143) and the p-value <.001clearly shows the significance of the model. Then it is evident that the variation explained by the model is statistically significant, and this suggests that the independent variables (Attitude, Subjective Norm, Perceived Behavioral Control, Habit and Regret), explain the level of Intention in complying with information security policies. The residual sum of squares 17.103 is lower than the regression sum of square 29.523 and this clearly shows that high level of intention variation is explained by the model. Then, the general ANOVA results shows that the regression model is validated.

4.6.3.1.2 Coefficients of predictor variables

Table 23 Model 1: Coefficient of predictor veriable

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	0.199	0.236		0.842	0.401
	Attitude	0.318	0.053	0.315	5.951	<.001

	SN	0.233	0.054	0.238	4.342	<.001
	PBC	0.348	0.056	0.343	6.180	<.001
	Reg	0.087	0.056	0.088	1.561	0.120
	Hab	0.070	0.053	0.074	1.315	0.190
a. Dependent Variable: Int						

Source: Self Survey (2026)

The contribution of each independent variable on intention is provided in the above coefficient table.

Among the predictors variable Perceived Behavioural Control shows the strongest positive effect which is (B = 0.348, Beta = 0.343, p = <.001), this indicates that employees who feels capable and confident of in their ability to comply with information security policy are significantly more likely to form an intention to comply with the Information Security Policy. Most employees feel capable of protecting their security and complying with information security policies in the company, that's why there is a strong and positive relation between PBC and intention.

Attitude also demonstrates a strong and statistically significant influence (B = 0.318, Beta = 0.315, p = <.001), indicating that employees who has a positive perceptions of security policies tend to show higher intention to comply. To be effective, compliance requires individual or personal acceptance not only enforcement. This strong significance happens because employees in the organization are internalizing it and not assuming it like a burden.

Subjective Norm likewise has a meaningful positive contribution (B = 0.233, Beta = 0.238, p = <.001), highlighting the role of social expectations or influence from others in shaping intentions. People tend to act based on what they assume others wat, it may be managers colleagues or other individuals in the company. This shows employees are influenced by others indicating that there is partial reinforcement on the behaviour to comply.

The study shows that regret does not have any impact on intention because it shows a value of (β = 0.088, p = 0.120) which produces clear results. The study shows that employees who think about their past compliance decisions will not change their future behavior according to their planned activities. The situation creates a conflict with

theoretical expectations which assume that regret will shape future behavior, although it is appropriate for this particular situation. People typically treat compliance work as their normal duties instead of viewing it as an intense personal decision. Compliance is not treated as personal choice with the assumption of consequence in the organization, but regret is free choice and self-blame Matarazzo et al. (2021). The situation requires emotional intensity which gives rise to regret, but this intensity does not exist in the current scenario. The study found that participants showed stable responses to regret items which showed moderate positivity, so this pattern reduced study variability while decreasing its ability to predict outcomes. The practical aspect of this situation indicates that organizations should not expect positive results when they attempt to change behavior through emotional appeals which connect to previous errors.

The same pattern occurs with habit because it fails to show any ability to forecast intention ($\beta = 0.074$, $p = 0.190$) just like other factors in the study. The situation creates an unexpected result because the descriptive data shows that people have high habit scores. The situation has two conditions because habits work automatically while intention requires active mental decision. Employees who make certain actions their daily practice will stop doing it. The model shows that habit does not produce any effect on intention. Even if employees have a strong habitual behaviour, their intention may be formed under defined rules not the habitual behaviours.

Generally, the coefficient analysis shows that cognitive and social factors particularly perceived behavioural control, Attitude and Subjective Norm influence Intention highly but Regret and Habit appear to be less direct in shaping employees' intention to comply with information security policies.

4.6.3.2 Information Security Policy Compliance Behavior (Model 2)

4.6.3.2.1 Model Summary

Table 24 Model 2: Model Summary

Model Summary[b]

				Change Statistics				
Model R	R Square	Adjusted R Square	Std. Error of the Estimate	R Square Change	F Change	df1	df2	Sig.F Change

1	.741[a]	.549	.544	.35530	.549	111.198	2	183	<.001

a. Predictors: (Constant), Int, PBC

b. Dependent Variable: ISP_Beh

Source: Self Survey (2026)

The above regression model shows that Information Security Policy Compliance Behavior is highly explained by the predictor variables (Perceived Behavioral and Intention) since the R^2 value is 0.549. This clearly tells that 54.9 % of the variance in Security Policy Compliance Behavior is explained by the above mentioned variables. Also, the model is significant (F = 111.198, p = <.001), which shows that the predictors collectively give a meaningful result as opposed to the result happening by chance and the general relationship also has a very strong value, as shown in the R value of 0.741. The model is stable and not overfit as the value of adjusted R^2 (0.544) is very close to the R^2, and the relative standard error which is 0.35530 tells that the predictions are fairly accurate. The above findings indicate that these behavioral variables have a significant and impact on the behavior of the employees toward adhering to information security policies.

4.6.3.2.2 ANOVA Test

Table 25 Model 2: ANOVA

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	28.075	2	14.037	111.198	<.001[b]
	Residual	23.101	183	.126		
	Total	51.176	185			

a. Dependent Variable: ISP_Beh

b. Predictors: (Constant), Int, PBC

Source: Self Survey (2026)

The general significance of the regression model on explaining Information Security Policy Compliance Behaviour is shown by the ANOVA results. The F value (111.198) and the p-value <.001clearly shows the significance of the model. Then it is evident that the variation explained by the model is statistically significant, and this suggests that the predictor variables (Perceived Behavioral Control and Intention), explain the level of Information Security Policy Compliance Behaviour. The residual sum of squares 23.101 is lower than the regression sum of square 28.075 and this clearly shows that high level of Information Security Policy Compliance Behaviour variation is explained by the model. Then, the general ANOVA results shows that the regression model is validated.

4.6.3.2.2 Coefficients of predictor variables

Table 26 Model 2: Coefficient of predictor variable

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	0.381	0.235		1.625	0.106
	PBC	0.434	0.069	0.409	6.257	<.001
	Int	0.426	0.068	0.407	6.232	<.001
a. Dependent Variable: ISP_Beh						

Source: Self Survey (2026)

The contribution of each predicted variable on Information Security Policy Compliance Behavior is provided in the above coefficient table.

Perceived Behavioral Control shows a positive effect which is (B = 0.434, Beta = 0.409, p = <.001), this indicates that employees who feels capable and confident of in their ability to comply with information security policy are significantly more likely to form a behavior to comply with the Information Security Policy. It is not merely an intention (high perceived behavioral control) but actually doing something regarding the information security behavior in this case, where the employees think they are confident to perform. In terms of practical implication, it can be interpreted that whenever perceived behavioral control score is higher or feel capable of controling security policies, employees are more likely to perform better in the information security

compliance behavior. This coefficient of perceived behavioral control in the model is also higher than the coefficient of intention which reiterates the point that perceived behavioral control is a motivator of behavior.

Intention also demonstrates a strong and statistically significant influence (B = 0.426, Beta = 0.407, p = <.001), suggesting that employees who have a clear intention to comply to ISP tend to translate that intention into real behaviour. Employees' determination to comply, depicted here by intention, naturally correlates with their subsequent behavior. Intention alone doesn't seem to affect behaviour, because even if employees are intended to follow but with out the confidence of capable of doing it, that intention can not fully applied into compliance behaviour.

4.7 Mediation Analysis

If zero is included in the confidence interval between upper and lower limit the indirect effect is non-significant, but if zero is not included the indirect effect is significant (Preacher,k.j & Hayes,F, 2004).

Table 27 Mediation Analysis

IV	Direct Effect (β, p)	Indirect Effect (β)	Boot CI	Mediation Type
Attitude	0.113, p = 0.044	0.077	[0.029, 0.129]	Partial
Subjective Norm	-0.080, p = 0.138	0.056	[0.018, 0.105]	Full
Perceived Behavioural Control	0.352, p = <.001	0.084	[0.029, 0.146]	Partial
Habit	0.406, p = <.001	0.017	[-0.009, 0.049]	Direct Effect (No Mediation)
Reg	0.039, p = 0.462	0.021	[-0.005, 0.058]	No Mediation

Source: Self Survey (2026)

Attitude Mediation

The result of meditation analysis shows a distinct illustration of how one of the TPB variable named attitude affects information security compliance behaviour through intention by analysing direct and indirect effects. While checking an effect of attitude on intention it has a strong and significant effect ($\beta = 0.318$, $t = 5.95$, $p < 0.001$), this clearly shows a strong path between attitude and the mediator intention and the indication is individuals with more positive attitudes toward information security policy

are more likely to develop a sturdy intention. Since intention also has a significant positive effect on information security policy compliance behaviour with (β = 0.241, t = 3.39, p = 0.001), it confirms path b and showing that Intention is crucial to mediate attitude into information security policy compliance behaviour.

When checking the direct effect attitude still have significant (β = 0.113, p = 0.044) effect even after including the mediator intention in the model, even if its significance is not strong compared to the indirect effect still it is significant. Also, the indirect effect of attitude on information security policy compliance behavior through intention is significant (β = 0.0766, BootCI [0.0285, 0.1294]), zero is not included in the confidence interval this verify that intention partially mediates the relationship between attitude and information security policy compliance behaviour.

In general, the above analysis shows that there is partial mediation, as information security policy compliance behaviour is affected by attitude both directly and indirectly through intention instead of functioning only by intention. This clearly stated that compliance behaviour is affected by both directly by employees' attitude to comply and their attitude through intention.

Subjective Norm Mediation

The result of meditation analysis shows a distinct illustration of how subjective norm affects information security compliance behavior through intention by analyzing direct and indirect effects. While checking an effect of subjective norm on intention it has a strong and significant effect (β = 0.233, t = 4.34, p < 0.001), this clearly shows individuals are more likely intended to comply with information security policy when the feel strong social pressure from their colleagues, managers etc. Since intention also has a significant positive effect on information security policy compliance behavior (β = 0.241, t = 3.39, p = 0.001), it confirms path b and showing that Intention is crucial to mediate subjective norm into information security policy compliance behavior.

When checking the direct effect subjective norm, it doesn't have a significant (β = -0.080, p = 0.138) effect even after including the mediator intention in the model, this shows that information security policy compliance is not directly affected by subjective norm. But, the indirect effect of subjective norm on information security policy compliance behavior through intention is positively significant (β = 0.0562, BootCI [0.0179, 0.1046]), zero is not included in the confidence interval this verify that

intention fully mediates the relationship between subjective norm and information security policy compliance behavior.

In general, the above analysis shows that a full mediation between subjective norm and information security policy compliance behaviour. This clearly indicated that social influence shape the employee's intention to comply with information security policy compliance instead of directly affecting compliance behaviour.

Perceived Behavioural Control Mediation

The result of meditation analysis shows a distinct illustration of how perceived behavioural control affects information security compliance behaviour through intention by analyzing direct and indirect effects. While checking an effect of PBC on intention it has a strong and positive significant effect ($\beta = 0.348$, $t = 6.18$, $p < 0.001$), this clearly shows a strong path between PBC and the mediator intention and the indication is individuals who feels capable and confident in their skill to comply with information security policy are more likely to develop a sturdy intention to comply. Since intention also has a significant positive effect on information security policy compliance behaviour with ($\beta = 0.241$, $t = 3.39$, $p = 0.001$), it confirms path b and showing that Intention is crucial to mediate PBC into information security policy compliance behaviour.

When checking the direct effect PBC still have significant ($\beta = 0.352$, $t = 5.97$, $p < 0.001$) effect even after including the mediator intention in the model. Also, the indirect effect of PBC on information security policy compliance behavior through intention is significant ($\beta = 0.0838$, BootCI [0.0291, 0.1464]), zero is not included in the confidence interval this verify that intention partially mediates the relationship between PBC and information security policy compliance behavior.

In general, the above analysis shows that there is partial mediation, as information security policy compliance behaviour is affected by PBC both directly and indirectly through intention instead of functioning only by intention, Iindicating that individuals are more likely to comply not only because they intend to, but also because they feel capable of doing so.

Habit Mediation

The result of meditation analysis shows a distinct illustration of how one of the TPB variable named attitude affects information security compliance behaviour through intention by analyzing direct and indirect effects. While checking an effect of habit on intention it doesn't have a significant effect ($\beta = 0.070$, $t = 1.31$, $p = 0.190$), this clearly shows that an intention to comply does not affected by habitual actions. Since intention has a significant positive effect on information security policy compliance behavior with ($\beta = 0.241$, $t = 3.39$, $p = 0.001$), it confirms path b and showing that Intention is crucial to mediate habit into information security policy compliance behavior.

When checking the direct effect attitude still have strong positive significant ($\beta = 0.406$, $t = 7.98$, $p < 0.001$) effect even after including the mediator intention in the model. The indirect effect of habit on information security policy compliance behavior through intention is not significant ($\beta = 0.0168$, BootCI [-0.0088, 0.0490]), zero is included in the confidence interval this verify that intention does not mediates the relationship between habit and information security policy compliance behavior.

In general, the above analysis shows that there is no mediation through intention, instead there is only direct relation between habit and information security policy compliance behaviour. This suggests that information security policy compliance driven by habit is more automatic and routine, rather than something that is consciously intended.

Regret Mediation

The result of meditation analysis shows a distinct illustration of how regret affects information security compliance behaviour through intention by analyzing direct and indirect effects. While checking an effect of regret on intention it doesn't have a significant effect ($\beta = 0.087$, $t = 1.56$, $p = 0.120$), this clearly shows that an intention to comply does not affected by regret. Since intention has a significant positive effect on information security policy compliance behavior with ($\beta = 0.241$, $t = 3.39$, $p = 0.001$), it confirms path b and showing that Intention is crucial to mediate habit into information security policy compliance behavior.

When checking the direct effect regret, it doesn't have a significant ($\beta = 0.039$, $p = 0.462$) effect even after including the mediator intention in the model, this shows that information security policy compliance is not directly affected by regret. Also, the indirect effect of regret on information security policy compliance behavior through

intention is not significant (β = 0.0209, BootCI [-0.0059, 0.0570]), zero is included in the confidence interval this verify that intention does not mediates the relationship between habit and information security policy compliance behavior.

The mediation results show that regret does not exert a significant indirect effect on information security policy compliance through intention, and it also does not have a significant direct effect on compliance behavior. This means that regret does not function as a meaningful explanatory pathway in the EthSwitch context. Although regret has been shown to strengthen compliance intentions in some earlier studies, such as Sommestad et al. (2015, 2019), the present findings suggest that its influence is limited in a highly regulated organizational setting where compliance is shaped more by formal rules, monitoring, and role-based expectations than by emotional anticipation.

A possible explanation is that employees at EthSwitch may not view security compliance as a personal decision that invites regret-based reflection. Instead, compliance appears to be embedded in routine work procedures and reinforced by organizational control systems. Under such conditions, the emotional weight of regret is likely reduced because employees are acting within clear institutional boundaries rather than making open-ended choices. This interpretation is also consistent with Matarazzo et al. (2021), who show that regret is shaped by how decision situations are experienced, rather than by a simple free-choice versus no-choice distinction.

In practical terms, this finding suggests that regret-based interventions may not be the most effective way to improve compliance in this setting. Efforts are more likely to be successful if they focus on strengthening employees' perceived behavioral control, clarifying expectations, and supporting consistent compliance routines. In other words, for EthSwitch, compliance seems to depend more on structure, capability, and organizational reinforcement than on anticipated regret.

4.8 Test of Hypothesis

H1: Attitude has a significant positive effect on employee's intention to comply with information security policy.

Attitude has a significant positive effect on employees' intention ($\beta = 0.315$, $p < 0.001$), the results shows that employees will have a strong intention to comply with information security if they have a positive attitude or perception about information security policy, so aspects of attitude will have a strong influence on intention to comply with information security policy. The result shows that it is aligned with prior literatures (Kuppusamy et al, 2022), Attitude shows a strong positive significance on intention to comply.

H2: Subjective norm has a significant positive effect on employee's intention to comply with information security policy.

Subjective norm also has a significant positive effect on employees' intention ($\beta = 0.238$, $p < 0.001$), the result shows that employees will have a strong intention to comply with information security policy if there is a social pressure from their colleagues, managers or others in their social circle. Even if it is not primary strong factor employees show the impact of subjective norm which is because employees are following what others benefited. Carmi.G (2021) suggests that subjective norm strongly affects intention to comply, which supports this paper finding.

H3: Perceived behavioural control has a significant positive effect on employee's intention to comply with information security policy.

Perceived behavioral control has a significant positive effect on employees' intention ($\beta = 0.343$, $p < 0.001$), the result shows that employees will have a strong intention to comply with information security policy when employees feels the are capable of complying or they feel like they have the skill to comply with information security policy. Individuals assumption about their capability towards security have a strong effect on their intention to comply (Infinedo ,2011).

H4: Habit has a significant positive effect on employee's intention to comply with information security policy.

Habit does not have a significant positive effect on employees' intention ($\beta = 0.074$, $p = 0.190$), this clearly shows that employee's intention to comply with information security policy compliance is not solely shaped by their past behavior or their habit. Even though a person does an action every day, that action does not necessarily force the compliance intention. Some studies establish a connection between habit and intention, while other studies prove that habit connects more closely to actual behavior

than to intention (Malimage ,2013). The study functions in this particular manner. The study shows that organizations should develop their employees' habitual patterns because this approach will directly boost compliance work even though it does not result in stronger intention.

H5: Regret has a significant positive effect on employee's intention to comply with information security policy.

Regret did not show a statistically significant positive effect on employees' intention to comply with information security policies (β=0.088,p=0.120), leading to the rejection of H5. Although this result is statistically clear, the more important issue is why regret failed to predict intention in this setting. One likely explanation is that compliance at EthSwitch is not experienced as a fully personal or discretionary choice. Instead, it is shaped by mandatory directives, hierarchical oversight, and routine organizational controls. In such a context, employees may comply because they are required to do so, not because they anticipate personal regret if they fail to comply.

This interpretation is consistent with the broader regret literature, which shows that regret is not only about free choice, but also about how decision situations are framed and experienced. Matarazzo et al. (2021) found that regret can still arise even in forced-choice situations, which means that the presence of regret depends on how personally salient and emotionally involving the decision feels, not simply on whether a choice exists. At EthSwitch, however, compliance may be too institutionalized and externally controlled for regret to work as a meaningful motivational factor.

The descriptive statistics also support this explanation. The regret items were already clustered at relatively high mean values with low dispersion, which suggests limited variation among respondents. When most employees already report fairly positive feelings about their past compliance decisions, regret has little room to differentiate between those who intend to comply and those who do not. In other words, regret may be present as a general sentiment, but it does not appear to function as a strong predictor of intention in this organization.

This finding contrasts with earlier studies. Sommestad et al. (2015) and Sommestad et al. (2019) reported that anticipated regret improved the explanatory power of TPB in Swedish organizational samples. Kuppusamy et al. (2022) also found that regret contributed positively to compliance intention in their organizational setting. The

difference suggests that regret is context dependent: it may matter more in settings where employees have greater personal discretion, but it becomes weaker in highly regulated environments where compliance is already embedded in formal rules and monitoring.

It is worth pausing here to look at the H4 and H5 results together and consider what they mean in light of the broader research landscape. Sommestad et al. (2015) found, in a Swedish organizational sample (n = 306), that anticipated regret significantly improved the prediction of compliance intention when added to the standard TPB framework. Their 2019 study (n = 645) replicated and extended this finding, showing both regret (+3.4% variance explained) and habit (+2.6%) made meaningful incremental contributions to intention. Kuppusamy et al. (2022) added regret as a TPB extension and similarly found it significant in predicting compliance intention. Against this backdrop, the rejection of H4 and H5 in this study is not simply a null result it is a substantive theoretical signal about what makes EthSwitch different from the organizational contexts where these extensions were found to work. The Swedish samples involved employees in high-income, institutionally mature environments with relatively decentralized decision-making around security compliance. At EthSwitch, the regulatory framework of the NBE and INSA essentially removes compliance from the domain of personal discretionary choice. As a result, neither the emotional motivation generated by anticipated regret nor the conscious intention reinforced by habitual routine appears to shape compliance intention in the same way. What does shape it strongly and significantly are perceived behavioral control, attitude, and subjective norm: the three core constructs of TPB that reflect institutional confidence, evaluative judgment, and social obligation. This pattern supports the conclusion that in mandatory compliance environments with clear external accountability structures, the rational-cognitive elements of TPB remain powerful, while the affective and habitual extensions lose their predictive leverage on intention specifically (though habit, importantly, retains a strong direct effect on behavior itself).

H6: Intention has a significant positive effect on employee's information security policy compliance behaviour.

Intention has a significant positive effect on employees' information security policy compliance behaviour ($\beta = 0.407$, $p < 0.001$), this indicates that employee's compliance behaviour towards an information security policy is strongly affected by employee's intention on information security policy. The theory by Alshammari (2025) suggests that intention has a positive strong effect on information security compliance behaviour. Interestingly though, the magnitude of the effect size being so close to perceived behavioral control indicates that intention and control are both equally influential here. This validates our belief that we should include perceived behavioral control as a behavioral factor and extends the theory to this specific context.

H7: Perceived Behavioural Control has a significant positive effect on employee's information security policy compliance behaviour.

Perceived behavioural control also has a significant positive effect on employees' information security policy compliance behaviour ($\beta = 0.409$, $p < 0.001$), this indicates that employee's compliance behaviour towards an information security policy is strongly affected by employee's believe that they are able to and can comply with the requirements of information security, it emphasizes that the ability to have the skill, resources and control of actions is as important as intention in motivating real behaviour. PBC has a direct effect on Information security policy compliance behavior (Alshammari 2025).

Table 28 Hyphothesis Test

Hypotheses Statement	**B**	**Sig.**	**Decision**
H1: Attitude has a significant positive effect on employee's intention	0.315	<0.001	Accepted
H2: Subjective norm has a significant positive effect on employee's intention.	0.238	<0.001	Accepted
H3: Perceived behavioural control has a significant positive effect on employee's intention.	0.343	<0.001	Accepted
H4: Habit has a significant positive effect on employee's intention.	0.074	0.19	Rejected
H5: Regret has a significant positive effect on employee's intention.	0.088	0.12	Rejected
H6: Intention has a significant positive effect on employee's information security policy compliance behavior.	0.407	<.001	Accepted

H7: Perceived Behavioral Control has a significant positive effect on employee's information security policy compliance behavior.	0.409	<.001	Accepted

Source: Self Survey (2026)

Chapter Five

Summary Conclusions and Recommendations

This chapter includes a conclusion and recommendations drawn from the analysis of behavioural factor (Attitude, Subjective norm, Perceived behavioural control, Habit and Regret) impact on Compliance behaviour.

5.1 Conclusion

The Pearson correlation shows that there are some significant relationships between the independent variables and information security compliance behaviour. The most significant positive correlation is with habit (r=0.687) and then perceived behavioral control (r =0.673) and intention(r=0.672). These data indicate that those with a high level of habit, perceived control, and intention are significantly more likely to demonstrate actual compliance behavior.

Similarly, moderate positive relationships are observed for attitude (r=0.511) and regret (r=0.509) with information security policy compliance behaviour. This indicates that the attitude toward the behavior and regret are involved in the mechanism of compliance with information security policy, but they are weaker than habit or perceived control relationships. The relationship for subjective norm (r=0.425) is somewhat weaker but still significant and positive. Therefore, all the behavioural variables examined showed positive and significant correlation with information security policy compliance.

The summary of regression model about causes of intention revealed that R2 = 0.633, which proves that this model can account for 63.3% of variation in the causes of intention. The strongest predictor is perceived behavioral control (β =0.343, p2.60.001), then attitude β (=0.315, p2.60.001) and subjective norm (β =0.238, p2.60.001). Thus, it can be concluded that the primary factors involved in intention formation are perceived behavioral control, attitude and subjective norm. Furthermore, habit (β =0.074, p=0.190), and regret (β =0.088, p=0.120) shows no significant influence on intention.

A regression analysis developed to evaluate compliance behavior indicated that combined intention and perceived behavioral control variables can explain 54.9% of information security practice compliance (R^2 = 0.549). Both predictor variables are significant. Perceived behavioral control is to some extent stronger (β = 0.409, p <

0.001) compared to intention ($\beta = 0.407$, $p < 0.001$), shows that when employees intended to follow information security policies and have the ability or skill to comply, they are more likely to have a positive compliance behaviour.

These relationships are also affected by the mediation of the variables. Intention is the partial mediator of attitude and perceived behavioral control variables. Also, intention fully mediates a relationship between subjective norm and compliance behaviour. But intention do not have a mediation effect on habit and regret at all. Habit has a direct effect on information security policy compliance behaviour. Regret do not have either a direct or indirect effect on compliance behaviour.

5.2 Theoretical Implication

The research study demonstrates an extension of Theory of Planned Behavior (TPB) through its integration of habit and regret to investigate information security policy compliance in financial institutions. The study results demonstrate that different predictors have different impacts on the outcome. Perceived behavioral control emerges as the strongest influence on intention and also shows a direct effect on actual compliance behavior, which proves that capability functions as the central element. Employees will comply with requirements when they believe that they possess the ability to do so. The relationship between control beliefs and both intention and behavior prove strong within this environment, which supports TPB's main argument.

Attitude and subjective norm also show significant effects on intention, which supports the traditional TPB structure. Employees who see security policies as positive and who feel social expectations around compliance are more likely to intend to follow them. The study results show that perceived behavioral control has stronger effects than their other variables. The theory receives an important additional aspect from this development. The study results show that internal organizational capacity has greater significance than personal assessment or social influence in determining employee intention within structured financial institution environments.

The non-significant effects of both habit and regret on compliance intention represent one of the more theoretically interesting findings of this study, and they deserve more than a brief acknowledgment. At first glance, these results seem to conflict with a growing body of evidence. Sommestad et al. (2015) showed, in a 306-person Swedish

organizational sample, that anticipated regret significantly improved prediction of compliance intention beyond the standard TPB constructs. In their 2019 follow-up with 645 white-collar workers, the same authors found regret increased explained variance by 3.4 percentage points and habit by an additional 2.6 points together raising the model's explanatory power by 5.4 percentage points. Kuppusamy et al. (2022) similarly found anticipated regret to be a significant predictor of compliance intention. These are serious empirical findings from peer-reviewed journals, so the question is not whether the extensions work in general the evidence says they can but why they do not appear to work here.

The answer almost certainly has to do with organizational context. The Swedish white-collar populations in the Sommestad studies operated within relatively flat, knowledge-driven organizations where information security compliance was largely treated as a personal responsibility. In those settings, employees made individual judgment calls about how closely to follow policies, and both the emotional weight of anticipated regret and the automatic pull of established habit naturally influenced those decisions. EthSwitch is structurally different. As Ethiopia's national interoperability switch, it operates under direct regulatory oversight from the National Bank of Ethiopia (NBE) and the Information Network Security Administration (INSA). Security policies at EthSwitch are not optional guidelines they are institutionally mandated, regularly audited, and embedded in employees' formal job responsibilities. In this kind of environment, the decision to comply is not a free personal choice in the way TPB extensions like regret assume. Where compliance is externally prescribed and monitored, that sense of personal agency and with it, the motivational force of anticipated regret is substantially diminished.

For habit, the picture is subtler. Habit did not predict intention ($\beta = 0.074$, $p = 0.190$), but it did show one of the strongest direct effects on compliance behavior in the entire model ($\beta = 0.406$, $p < 0.001$). This pattern is consistent with what Limayem et al. (2007) described as the "habit–intention gap": when behaviors become sufficiently automatized through repeated performance, they begin to bypass deliberate intention and instead influence action through a separate automatic pathway. Put more simply, employees who have genuinely internalized security routines tend to comply not because they consciously decide to each time, but because the behavior has become second nature. This means that if organizations only target intention-building through

awareness campaigns and policy communication they may miss the deeper compliance gains available through habitual routine formation. The finding that habit's influence runs directly to behavior rather than through intention is therefore not a failure of the extended TPB model; it is a theoretically coherent result that reveals something important about how compliance works in structured, high-frequency task environments like EthSwitch. Taken together, these findings suggest that the practical relevance of TPB extensions depends heavily on the institutional setting in which they are tested, and that researchers should treat organizational context as a moderating variable rather than an afterthought when applying behavioral models to information security compliance.

Third, the finding that intention substantially increased the prediction of behaviors confirms TPB's basic assumption. Meanwhile, the substantial direct effect of perceived behavioral control on behavior, close in magnitude to that of intention, further enhances TPB's theoretic contribution. While intention was obtained, actual employee behaviors largely relied on employees' degree of perceived capability to act. In sum, this research supports TPB while emphasizes the power of perceived behavioral control and diminishing role of habit and regret in predicting intention.

5.3 Recommendations

In accordance with the findings and analysis on the behavioural factors influencing the Information Security Policy Compliance, the following are the recommendations that can be used for further enhancements and establishment of a stronger security policy compliance behaviour in the organization.

- Ethswitch should focus on improving its employee's capability, skill, competence and potential since Perceived behavioural control highly associated with intention and information security policy compliance behaviour. By giving employees adequate technical awareness and assistance, giving clear guidance and letting easy to use system, companies can benefit since, employees develop a confidence on their capability to comply with information security policy.
- Ethswitch must focus on enhancing its employee's intention towards information security policy compliance behaviour as intention has a strong positive significance on compliance behaviour. This can be achieved by regular and targeted awareness session about security policies, creating simple and clear

security policies, introduce incentive or recognition for those who follow the policies and clearly communicate the benefit of compliance toward information security policies. Letting understand employees why they follow compliance rule instead of just only waiting them to do it will strength employees' intention to comply.

- The significant effect of Attitude on employee's intention to comply with information security policies indicates that employs will follow security policies when they have a positive attitude or perception about the policies, So Ethswitch should focus in creating and shaping a positive employees perception towards information security policies. It can be achieved through emphasizing the advantages of compliance, providing real-life examples of security risks, and making the policies more practical and relevant to employees in their day-to-day operations.
- The intention towards information security policy compliance is strongly influenced by Subjective Norm, this shows that social or subjective norm importance in security policy compliance. Top management and every employee must follow and drive compliance. Employees intention affected by their management and colleague way of compliance. So, Ethswitch should strictly follow top management and all employee's compliance culture since it has a direct strong effect on other employee's compliance intention.
- Ethswitch should rely on more preventive and supportive strategies since regret doesn't affect intention and compliance behaviour. So, the company must emphasize on giving employees guidance, training or positive reinforcement instead of focusing on improvement of negative consequences regret.
- Ethswitch need to establish ongoing and regular monitoring mechanism on information security compliance behaviour which will check compliance activities and measure its security program effectiveness, it may be done through arranging different feedback mechanism, periodic assessment and performance indicator of compliance to follow the progress since these methods helps identifying the gaps and show gaps to be improved.

The findings suggest that EthSwitch should move beyond general awareness campaigns and adopt more targeted compliance interventions. Since attitude, subjective norm, and perceived behavioral control showed stronger effects than regret, management should

focus on making compliance easier, clearer, and more visible in daily work. For example, the organization can introduce security behavior nudges, such as timely reminders during sensitive tasks, short in-system prompts before risky actions, and role-based compliance messages tailored to each department.

In addition, a gamified compliance program could be used to make security practices more engaging and measurable. Employees could earn recognition points for consistent compliance, timely completion of security tasks, or participation in policy refreshers. This kind of approach may help turn compliance from a routine obligation into a more active organizational habit.

EthSwitch may also benefit from behavioral analytics and continuous compliance dashboards that give managers a real-time view of compliance trends, policy violations, and training gaps. Rather than relying only on occasional audits, such tools would allow the organization to identify weak points early and respond before problems escalate. Overall, the study suggests that sustainable ISP compliance is more likely to improve when the organization combines structural support, behavioral cues, and continuous feedback instead of relying only on general awareness messages.

The organization can achieve better information security policy compliance while decreasing potential risks through its focus on employee skills and work habits and its efforts to build better organizational backing and effective communication systems.

5.4 Recommendation for Management

The management team needs to create compliance requirements which employees can easily fulfill without needing to fulfill mandatory obligations. The research demonstrates that employee compliance increases when employees believe they have sufficient capabilities therefore training must include both theoretical knowledge and practical execution of tasks. Employees must receive complete instructions about implementing security policies into their daily duties instead of learning only the policy content. The same level of importance exists for both procedure streamlining and process simplification. Any employee who wants to follow policies will find it impossible to do so when the policies become excessive in complexity or demand too much time. The combination of clear steps together with basic instructions and assistance tools will help decrease this resistance. The organization needs to keep showing commitment to security through executive backing which creates a workplace

atmosphere where security compliance becomes standard procedure instead of an additional work obligation.

5.5 Strategic and Organizational Recommendations

The National Bank of Ethiopia (NBE) needs to change its regulatory approach by shifting from basic policy verification to actual policy implementation assessment. The evaluation process requires assessment of the training quality together with determination of actual employee operational compliance capabilities. The assessment requirements need to become public while organizations must show performance through assessment tests and real experience evaluations. The financial sector needs standardized practices which should include security training requirements and competency assessment standards because these will help maintain uniformity between financial organizations. The industry needs enforcement to succeed but institutions must receive assistance in developing their workforce through established guidelines and shared information about successful methods which will create lasting compliance solutions.

5.6 Limitation of the study

Even though the study offers helpful insight, on factors affecting information security policy compliance, below limitations should be considered.

- A further limitation of this study concerns the interpretation of directional relationships. Although the regression analyses identify statistically significant associations between the predictor variables and compliance outcomes, the cross-sectional design of this study does not permit causal inference in the strict experimental sense. The language of "effect" and "influence" used throughout this thesis reflects the directional predictions of TPB and the hypothesized theoretical relationships as is common in behavioral survey research (Ajzen, 1991; Sommestad et al., 2019) rather than claims of experimentally verified causality.
- The study focus was based only financial area that creates lack of generalizability to other industries and also it is limited to specific financial company.

5.7 Recommendation for future research

- Future studies may consider using mixed approach which is both qualitative and quantitative, since qualitative methods like interviews or focus group discussions could offer deeper insights into why employees behave the way they do.
- In addition to behavioural factors future studies could widen the scope to other factors like organizational cultures, technologies security security awareness to get more comprehensive view of what drives compliance behavior in organizational settings.
- Future research should adapt longitudinal designs methods to measure changes in behavior over time, especially as organizations introduce new technologies, policies, or training programs. employing longitudinal or experimental designs would strengthen the causal interpretation of these findings.
- Future studies should apply this research across different sectors such as healthcare, education, telecommunications, and government agencies.
- This study target population was only Ethswitch employees, but to have a relevant data from different source the researcher better include populations from member financial institutions since their compliance behavior affect the company.

Reference

Abay, A & Lessa, L & Negash, S. (2022). BANK INFORMATION SYSTEMS VULNERABILITY: THE CASE OFETHIOPIA. School of Informa□on Science, Addis Ababa University, Ethiopia, https://www.researchgate.net/publication/363517964_BANK_INFORMATION_SYSTEMS_VULNERABILITY_THE_CASE_OF_ETHIOPIA

Abebe, G., & Lessa, L. (2020). Human factors influence in information systems security: Towards a conceptual framework. In Proceedings of the 2nd African International Conference on Industrial Engineering and Operations Management (pp. 2207-2216). IEOM Society International. http://www.ieomsociety.org/harare2020/papers/500.pdf

Ahmad, M. R., Osman, M. H., Abdullah, A., & Sharif, K. Y. (2024). Evolution of Information Security Awareness towards Maturity: A Systematic Review. International Journal on Advanced Science Engineering Information Technology, 14(5), 1738-1747. https://doi.org/10.18517/ijaseit.14.5.20234

Ahmad, N., Alias, F. A., Hamat, M., & Mohamed, S. A. (2024). Reliability analysis: Application of Cronbach's alpha in research instruments. In SIG e-Learning@CS proceedings (pp. 114–119). Universiti Teknologi MARA Cawangan Pulau Pinang. https://appspenang.uitm.edu.my/sigcs/2024-2/Articles/20244_ReliabilityAnalysis-ApplicationOfCronbachsAlphaInResearchInstruments.pdf

Aimero, B. (2023). THE EFFECTS OF CYBER-ATTACKS ON BANKS BUSINESS ICT SYSTEMS: THE CASE OF BANKS IN ETHIOPIA. ST. MARY'S UNIVERSITY SCHOOL OF BUSINESS. DOI:10.13140/RG.2.2.18169.28001

Ajezen, I. (1991). The Theory of Planned Behavior. ORGANIZATIONAL BEHAVIOR AND HUMAN DECISION PROCESSES, 50, 179-211. DOI:10.1016/0749-5978(91)90020-T

Almansoori, A & Al-Emran, M & Shaalan, K. (2023). A Systematic Review of Studies and Theories. Applied Science, 13, 5700. Theories. Appl. Sci. https://doi.org/10.3390/app13095700

Alqahtani, M & Braun, R. (2021). Reviewing Influence of UTAUT2 Factors on Cyber Security Compliance: A Literature Review. Journal of Information Assurance & Cyber security, 2021, 15. DOI: 10.5171/2021.666987

Alshammari, M.M.& Al-Mamary, Y.H. (2025). Bridging Policy and Practice: Integrated Model for Investigating Behavioral Influences on Information Security Policy Compliance. Systems , 13, 630. https://doi.org/10.3390/systems13080630

Alzahrani, L. (2021). Factors Impacting Users' Compliance with Information Security Policies: An Empirical Study. International Journal of Advanced Computer Science and Applications, 12(10), 437-447. https://thesai.org/Downloads/Volume12No10/Paper_49-Factors_Impacting_Users_Compliance_with_Information_Security.pdf

ARMAUER HANSEN RESEARCH INSTITUTE. (2021). Information Systems Security Policy and Procedure. Information Systems Security Policies and Procedures, 1. ahri.gov.et/storage/2020/12/AHRI-ISSPP-v1.0-Information-System-Security-Policy-and-Procedure-Final.pdf

Ashenafi, E. (2025). Fragmented Cybersecurity Approach Threatens Ethiopia's Digital Payment System. The Reporter. https://www.thereporterethiopia.com/48148/

Assefa, T & Tensay, A. (2021). Factors influencing information security compliance: an institutional perspective. College of Natural and Computational Sciences, Addis Ababa University, 44(1), 108–118. DOI: https://dx.doi.org/10.4314/sinet.v44i1.10

Bauer, S., & Bernroider, E. W. N. (2017). From information security awareness to reasoned compliant action: Analyzing information security policy compliance in a large banking organization. The DATA BASE for Advances in Information Systems, 48(3), 44–68. https://doi.org/10.1145/3130670.3130674

Brehaut, J. C., O'Connor, A. M., Wood, T. J., Hack, T. F., Siminoff, L., Gordon, E., & Feldman-Stewart, D. (2003). Validation of a decision regret scale. *Medical Decision Making, 23*(4), 281–292. https://doi.org/10.1177/0272989X03256005

Bulgurcu, B., Cavusoglu, H. and 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. doi:10.2307/25750690

Carmi, G., & Bouhnik, D. (2021). Behavioral factors that influence employees to comply with information security policies. *Journal of Internet Technology and Secured Transactions (JITS), 9*(1). https://infonomics-society.org/wp-content/uploads/Behavioral-Factors-That-Influence-Employees.pdf

Chen, H. C., Lin, S. Y., & Chen, I. H. (2022). Better safe than sorry: The role of anticipated regret and organizational ethical climate in predicting workplace safety behavior. Chinese Management Studies, 18(1), 48–70. https://doi.org/10.1108/CMS-10-2021-0446

Creswell, J. W. (2014). Research Design: Qualitative, Quantitative and Mixed Methods Approaches. Canadian Center of Science and Education, 12(5). https://doi.org/10.5539/elt.v12n5p40

Delso-Vicente, A & Diaz Marcos, L & Aguado Tevar, O & Blanes Sebastián, M. (2025). Factors influencing employee compliance with information security policies: a systematic literature review of behavioral and technological aspects in cybersecurity. Future Business Journal, 11(28). https://doi.org/10.1186/s43093-025-00452-7

Fagade, T. & Tryfonas, T. (2016). Security by Compliance? A Study of Insider Threat Implications for Nigerian Banks. Human Aspects of Information Security, Privacy, and Trust, 9750, 128-139. https://doi.org/10.1007/978-3-319-39381-0_12

Ganapati, S & Ahn, M & Reddic, C. (2023). Evolution of Cybersecurity Concerns: A Systematic Literature Review. , K. (2023I). Exploring the Frontiers of Cybersecurity Behavior:. Applied Science, 13, 5700. https://doi.oTheories. Appl. Sci. 2023, 13, 5700.https://doi.org/10.3390/

Huy, S., Ang, S., Ho, M., & Balasubramaniam, V. (2025). Insider Threats in Banking Sector: Detection, Prevention, and Mitigation. Journal of Cyber Security and Risk Auditing, 2025(4), 257–265. https://doi.org/10.63180/jcsra.thestap.2025.4.5

Hwang, I & Seo, R & Hu, S. (2025). Boosting employee information security compliance: the contingent roles of task–technology and person–organization fits. HUMANITIES AND SOCIAL SCIENCES COMMUNICATIONS, 12, 563, https://doi.org/10.1057/s41599-025-04718-x

Ifinedo, P. (2011). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), 83-95, DOI:10.1016/j.cose.2011.10.007

Islam, M. S., & Xiangdong, L. (2024). Guardians of the web: The evolution and future of website information security. arXiv. https://doi.org/10.48550/arXiv.2505.04308

Izah, S. C., Sylva, L., & Hait, M. (2024). Cronbach's alpha: A cornerstone in ensuring reliability and validity in environmental health assessment. ES Energy & Environment, 23, Article 1057. https://espublisher.com/uploads/article_pdf/esee1057.pdf

Kalam, K. & Abu Barkat Ullah. (2025). Human factors in cybersecurity: an interdisciplinary review and framework proposal. International Journal of Information Security, 24(3),119. https://doi.org/10.1007/s10207-025-01032-0

Kuppusamy, P., Samy, G. N., Maarop, N., Shanmugam, B., & Perumal, S. (2022). Information security policy compliance behavior models, theories, and influencing factors: A systematic literature review. *Journal of Theoretical and Applied Information Technology*,*100*(5),1535–1556.
https://www.jatit.org/volumes/Vol100No5/28Vol100No5.pdf

Lessa, L & Gebrehawariat, D. (2023). Effectiveness of banking card security in the Ethiopian financial sector: PCI-DSS security standard as a lens. International Journal of Industrial Engineering and Operations Management, 5(2), 135-147. DOI 10.1108/IJIEOM-10-2021-0015

Liang, H., & Xue, Y. (2021). Protection motivation theory in information systems security research: A review of the past and a roadmap for the future. ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 52(2), 9–28. https://doi.org/10.1145/3462766.3462770

Limayem, M., Hirt, S. G., & Cheung, C. M. K. (2007). How habit limits the predictive power of intention: The case of information systems continuance. *MIS Quarterly, 31*(4), 705–737. https://doi.org/10.2307/25148817

Lubua, E & Semlambo, A & Mkude, C. (2022). Factors Affecting the Security of Information Systems in Africa: A Literature Review. University of Dar es Salaam Library Journal, 17(2), 94-114. https://dx.doi.org/10.4314/udslj.v17i2.7

Malimage, Kalana, "The Role of Habit in Information Security Behaviors" (2013). Theses and Dissertations. 4635. https://scholarsjunction.msstate.edu/td/4635

Matarazzo O, Abbamonte L, Greco C, Pizzini B and Nigro G (2021) Regret and Other Emotions Related to Decision-Making: Antecedents, Appraisals, and Phenomenological Aspects. Front. Psychol. 12:783248. doi: 10.3389/fpsyg.2021.783248

Mishra, A & Alzoubi, Y.I & Gill, A.Q & Anwar, M.J. (2022). Cybersecurity Enterprises Policies: A Comparative Study. Sensors, 22, 538. https://doi.org/10.3390/s22020538

Mohamud, A,j & Rahman, TK. (2024). Impact of Information Security Policies Compliance (ISPC) on Reducing the Incidence of Security Breaches in Organizations: Systematic Literature Review, Preprints.org, 1. doi: 10.20944/preprints202409.1715.v1

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly, 42*(1), 285–311. https://doi.org/10.25300/MISQ/2018/13853

Narasimha, S. (2020). EVALUATING INFORMATION SECURITY AWARENESS AND COMPLIANCE IN SUB-SAHARAN AFRICA: AN INTERPRETIVIST PERSPECTIVE. 13th IADIS International Conference Information Systems, 187-190. https://www.academia.edu/115012071/Evaluating_Information_Security_Awareness_and_Compliance_in_Sub_Saharan_Africa_An_Interpretivist_Perspective

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). An introduction to information security (NIST Special Publication 800-12 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-12r1

Nord, J. H., Koohang, A., Floyd, K., & Paliszkiewicz, J. (2020). Impact of habits on information security policy compliance. *Issues in Information Systems, 21*(3), 217–226. https://doi.org/10.48009/3_iis_2020_217-226

Nunnally, J. C. (1978). *Psychometric theory* (2nd ed.). McGraw-Hill. Nunnally, J. C. (1978). *Psychometric theory* (2nd ed.). McGraw-Hill.

Ogbanufe, O & Baham, C. (2023). Using Multi Factor Authentication for Online Account Security: Examining the Influence of Anticipated Regret. Information Systems Frontiers, 25, 897–916. https://doi.org/10.1007/s10796-022-10278-1

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. Journal of Applied Psychology, 88(5), 879–903. https://doi.org/10.1037/0021-9010.88.5.879

Preacher, K. J., & Hayes, A. F. (2004). SPSS and SAS procedures for estimating indirect effects in simple mediation models. Behavior Research Methods, Instruments, & Computers, 36(4), 717–731. https://doi.org/10.3758/BF03206553

Putri Maharani Akib, A & Candiwan, C & Puteri Ramadhani, D. (2025). Cybersecurity Compliance and Other Factors Influencing Employee Protective Behavior: A Case Study of Bank X in Indonesia. International Journal of Safety and Security Engineering, 15(6), 1229-1241. https://doi.org/10.18280/ijsse.150613

Shimels, T & Lessa, L. (2022). Maturity of information systems' security in Ethiopian banks: case of selected private banks. International Journal of Industrial Engineering and Operations Management, 5(2), 86-103. DOI 10.1108/IJIEOM-10-2021-0014

Shimels, T & Lessa, L. (2023). Maturity of information systems' security in Ethiopian banks: case of selected private banks. International Journal of Industrial Engineering and Operations Managemen, 5(2), 86-103. DOI 10.1108/IJIEOM-10-2021-0014

Sommestad, T & Karlzén, H & Hallberg, J. (2019). The sufficiency of the theory of planned behavior for explaining information security policy compliance. Information and Computer Security 23(2), 200-217, DOI:10.1108/ICS-04-2014-0025

Sommestad, T & Karlzén, H & Hallberg, J. (2019). The Theory of Planned Behavior and Information Security Policy Compliance. ournal of Computer Information Systems, 59(4), 344-353. https://doi.org/10.1080/08874417.2017.1368421

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. Computers & Security, 109, Article 102387. https://doi.org/10.1016/j.cose.2021.102387

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. Information & Management, 49(3), 190–198. https://doi.org/10.1016/j.im.2012.02.002

Vance, A., Siponen, M., & Straub, D. W. (2020). Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures. Information & Management, 57(8), 103322. https://doi.org/10.1016/j.im.2020.103322

Weickert, T. D., Joinson, A., & Craggs, B. (2023). Is cybersecurity research missing a trick? Integrating insights from the psychology of habit into research and practice. Computers & Security, 128, Article 103130. https://doi.org/10.1016/j.cose.2023.103130

Woretaw, A & Lessa, L. (2019). Factors Hindering Full-Fledged Information Security in Banking Sector in Ethiopia: Emphasis on Information Security Culture. Twenty-fifth Americas Conference on Information Systems, Cancun. https://www.academia.edu/43975222/factors_Hindering_Full_Fledged_Information_Security_in_Banking_Sector_in_Ethiopia_Emphasis_on_Information_Security_Culture

World Bank. (2025). Cyber risks in fast payment systems (Focus Note). International Bank for Reconstruction and Development / The World Bank. https://fastpayments.worldbank.org/sites/default/files/2025-02/Cybersecurity%20Focus%20Note_Feb%2019_Final.pdf

Zamil, M. H., & Faruq, M. O. (2022). Cybersecurity and data integrity in financial systems: A review of risk mitigation and compliance models. International Journal of Scientific Interdisciplinary Research, 1(1), 27–61. https://doi.org/10.63125/azwznv07

APPENDIX

Appendix 1: Research Questionnaire

Dear Respondent,

I am conducting this research for my thesis requirement. The study aims to understand how behavioural factors influence employee compliance with information security policies here at Ethswitch.

Research Goal

This study examines how attitudes, social pressures, perceived control, habits, and regret affect the way employees comply with information security policies. The findings may help financial institutions in Ethiopia better understand the human side of security compliance.

Confidentiality

- Your responses are completely anonymous. No names, Email address or employee IDs are required.
- Data will be used for academic purposes only.
- Individual responses will not be shared with anyone at Ethswitch. Only group findings will be presented.

Thank you for your time and honest input.

Section 1: Demographic factor

Gender

□ Male

□ Female

Age

□ Below 25

□ 25-34

□ 35-44

□ 45-54

□ 55 and above

Education Level

□ High School

□ Bachelors Degree

□ Masters Degree

□ PHD

Years of experience at Ethswitch

□ less than 1 year

□ 1-3 years

□ 4-5 years

□ 6-8 years

□ Greater than 9 years

Job Role Under

□ CIO(Chief Information Officer)

□ COO(Chief Operation Officer)

□ CCO(Chief Corporate Officer)

□ CPO(Chief Portfolio Officer)

Section 2: Attitude

(Likert Scale: 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree)

	Questions	1	2	3	4	5
1	I feel that compliance with the Information Security Policy (ISP) is a positive thing.					
2	I feel that compliance with the ISP is reasonable.					
3	I feel that compliance with the ISP is important.					
4	Following the Information Security Policy is a good idea.					

5	Following the Information Security Policy is pleasant.					

Section 3: Subjective Norms

(Likert Scale: 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree)

	Questions	1	2	3	4	5
1	Top management believes I should comply with the organization's information security policies.					
2	My boss believes I should comply with the organization's information security policies.					
3	My colleagues believe I should comply with the organization's information security policies.					
4	The information security department in my organization believes I should comply with information security policies.					
5	Other technical computer specialists in the organization believe I should comply with information security policies.					

Section 4: Perceived Behavioral Control

(Likert Scale: 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree)

	Questions	1	2	3	4	5
1	I have the necessary skills to comply with the organization's Information Security Policy (ISP).					
2	I have the expertise to implement preventive measures, in line with the ISP, to protect my confidential information and organizational computers from harm.					
3	I believe it is within my control to comply with the Information Security Policy (ISP).					
4	For me, following the security procedures described in the Information Security Policy (ISP) is easy.					
5	My ability to comply with the Information Security Policy (ISP) and prevent security violations is adequate.					

Section 5: Habit

(Likert Scale: 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree)

	Questions	1	2	3	4	5
1	Complying with information security policies is something I do frequently.					
2	Complying with information security policies is something I do automatically.					
3	Complying with information security policies is something I do without having to consciously remember to do so.					
4	Complying with information security policies is something that belongs to my routine.					
5	Complying with information security policies is something I would find hard not to do.					

Section 6: Regret

(Likert Scale: 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree)

	Questions	1	2	3	4	5
1	Following the information security policy was the right decision					
2	I didn't regret the way I complied to the information security policy					
3	I would follow the same compliance decision regarding the information security policy again					
4	My decision regarding the information security policy caused positive consequences					
5	My decision regarding the information security policy was wise					

Section 7: Intention

(Likert Scale: 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree)

	Questions	1	2	3	4	5
1	I am likely to comply with my organization's information security policies.					
2	It is possible that I will follow information security policies to help protect the organization's information systems.					
3	I am certain that I will act in accordance with the organization's information security policies.					
4	I intend to comply with the requirements of my organization's Information Security Policy (ISP) in the future.					
5	I intend to safeguard information and technology resources and carry out my assigned responsibilities as outlined in the ISP when using organizational information and technology.					

Section 8: compliance with the Information Security Policy (ISP)

(Likert Scale: 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree)

	Questions	1	2	3	4	5
1	I comply with the Information Security Policy (ISP).					
2	I recommend that others comply with the Information Security Policy (ISP).					
3	I assist others in complying with the Information Security Policy (ISP).					
4	I follow the security procedures described in the Information Security Policy (ISP).					
5	I apply the requirements of the Information Security Policy (ISP) when using organizational information and technology.					