A FRAMEWORK FOR ENHANCING INFORMATION SYSTEMS SECURITY AMONG SMALL ENTERPRISES IN UGANDA

A dissertation presented to

FACULTY OF SCIENCE

in partial fulfillment of the requirements for the award of the degree

Master of Science in Information Systems

UGANDA MARTYRS UNIVERSITY

JIMMY Musinguzi

2023-M312-21504

Supervisor: Brian Kasozi

August 2025

UGANDA MARTYRS UNIVERSITY

DIRECTORATE OF GRADUATE STUDIES, RESEARCH AND ENTERPRISE

Master's Dissertation

Declaration

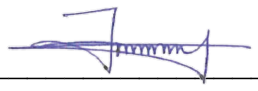
I have read the rules of Uganda Martyrs University on plagiarism and academic honesty, and hereby state that this work is my own.

It has not been submitted to any other institution for another degree or qualification, either in full or in part.

Throughout the work I have acknowledged all sources used in its compilation.

I finally grant Uganda Martyrs University permission to store and reproduce this dissertation, in whole or in part, in any manner or format, which Uganda Martyrs University may deem fit.

Researcher's name: Jimmy Musinguzi

Researcher's signature: 

Date of submission: 30/08/2025

Submitted to the Directorate of Graduate Studies, Research and Enterprise

UGANDA MARTYRS UNIVERSITY

DIRECTORATE OF GRADUATE STUDIES, RESEARCH AND ENTERPRISE

Master's Dissertation

Approval

This dissertation has been produced under my/our supervision and submitted for examination with my/our approval as the appointed academic supervisor/s.

Name of Supervisor Brian Kasozi

Signature of Supervisor: _____

Date of submission: 30/08/2025

Submitted to the Directorate of Graduate Studies, Research and Enterprise

DEDICATION

This work is dedicated to my Late Mother Mary Kabonesa Amooti and my Dad Mathias K Matovu Adyeeri whose visionary thoughts and belief in me have driven me to attain and achieve a better quality of excellence.

ACKNOWLEDGEMENT

I am greatly indebted to my lovely family for their support and encouragement. Without you this would have been a difficult journey to navigate.

Foremost, I would like to express my gratitude to my supervisor, Mr. Brian Kasozi, for his support and excellent advice. I am grateful for his support and invaluable contributions to this research.

I would like to thank John Jordan, Stephen Lok and the ED & F Man Commodities Technology team for their support. Their expert advice has given me a safe space to post about my journeys and my struggles.

The author would also like to thank the Department of Computer Science & Information Systems for their support and invaluable advice during the panel presentations.

Thank you for all the hilarious, great insight and contributions.

LIST OF ABBREVIATIONS

SEs	Small Enterprises
InfoSec	Information Security
NITA-U	National Information Technology Authority – Uganda
NIST	National Institute of Standards and Technology
CSF	Cyber security framework
ISS	Information systems security
TPS	Transaction Processing Systems
DSR	Design Science Research
CRM	Customer Relationship Management
ERP	Enterprise Resource Planning
DSS	Decision Support Systems
ISSP	Information Systems Security Program
BYOD	Bring your own device
NDA	Non-disclosure agreement

DEFINITION OF TERMS

Information systems security: The protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats (CSRC, n.d.).

Information security: "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability" (Paulsen & Toth, 2016)

Cyber security: "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation" (Paulsen & Toth, 2016)

Security Framework: is a collection of well-documented standards, policies, procedures and best practices intended to strengthen an organization's security posture and reduce risk (CyberArk, n.d.).

Small enterprise: an enterprise employing between 5 and 49 people and having total assets between UGX10 million but not exceeding 100 million (UIA, n.d.).

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

Over the past decade, there has been a sharp increase in the number of small enterprises adopting digital technologies in the quest for improving efficiency and competitiveness. This is majorly attributed to the expansion of the IT infrastructure, mobile money and covid-19 pandemic. However, this dependence on digital technologies exposes the small businesses to a vast array of cyber threats such as phishing, ransomware, and fraud, against which they remain highly vulnerable. A major challenge is the lack of a tailored information systems security framework addressing the unique needs and constraints of small enterprises. Existing national frameworks (like the NITA-U National Information Security Framework) are geared toward larger organizations, leaving small enterprises with guidelines that are too generic, complex, and costly for them to implement. Resource limitations and minimal in-house expertise further exacerbate the security gaps for small enterprises.

This research applies a Design Science Research (DSR) methodology to address the problem by designing and validating an artifact, a customized Information Systems Security (ISS) framework for Ugandan small enterprises. Following the DSR paradigm, the study first identifies and clarifies the practical problem and motivates the need for a solution. It then defines the objectives for a feasible security solution tailored to small businesses. Guided by these objectives and informed by a review of existing frameworks and empirical data, a security framework artifact was designed. The artifact was iteratively refined through demonstration and evaluation: an initial version of the framework was presented to practitioners for feedback, and a formal evaluation was conducted via expert reviews to assess its effectiveness in improving security for small enterprises. The final stage involved communication of the results and artifact, as captured in this thesis.

The resulting framework is a practical, four-phased security management model that aligns with industry best practices (drawing on NISTIR 7621 and ISO 27001 standards) while remaining lightweight and affordable for small businesses. It emphasizes a cycle of continuous improvement through phases of assessment, planning, implementation, and monitoring, each with specific actionable measures attuned to the resource constraints of Ugandan small enterprises. Evaluation findings show that the framework is well-aligned with the needs of small enterprises as it addresses identified security gaps, is cost-conscious by leveraging existing tools and guidelines, and is adaptable to the local context. The expert validation confirmed the artifact’s relevance and effectiveness, providing confidence that adopting the framework can significantly bolster the information security posture of small enterprises.

In summary, this study contributes in two main ways: (1) it provides a validated security framework that small businesses can easily use to improve their information systems security, and (2) it offers insights from design science on creating security solutions tailored to specific contexts. This shows how design science research can connect general best practices with the needs of local organizations. This work not only provides a valuable solution for practitioners in Uganda's small business sector but also enhances academic understanding by showing how global security frameworks can be adapted to fit the needs of local small enterprises through a detailed design science approach

CHAPTER ONE
INTRODUCTION

1.1 Overview

Small enterprises are increasingly adopting digital technologies for daily business operations and customer services. Major milestones such as the explosion of mobile money services, expansion of internet infrastructure, and the COVID-19 pandemic can be attributed to the accelerated digital uptake. However, the dependence on information systems has exposed small enterprises to growing cyber threats. This section explores information security best practices and the unique vulnerabilities faced by small enterprises in Uganda.

1.2 Background

Amidst the wave of digital technology, data has become the lifeblood of all businesses in the quest for business continuity and operational efficiency (Wadie & Ahuja, 2025). Small enterprises play a vital role in driving economic growth in developing countries and in the quest for success and long-term survival, these have been forced to adopt digital technologies (Papathanasiou, et al., 2024). With heavy dependency on information systems, handling sensitive data and customer information, information security threats have skyrocketed hence making information security a great concern for these businesses (SecurDI, 2023).

Enterprises and in particular small enterprises often encounter unique information security challenges emanating from limited resources and expertise. Most small enterprises often rely on outsourced IT services due to lack of dedicated IT departments which end up introducing more vulnerabilities (SecurDI, 2023).

Quite often, small enterprises do not see a return on investment by investing in IT hence prioritize business operations over information security thus becoming attractive targets for cybercriminals. Any lapse in information security best practices increases the susceptibility of small enterprises to information security threats such as data breaches, unauthorized access attempts, phishing attacks, malware infections, ransomware attacks, denial of service attacks among others. Such threats can lead to data loss, financial losses, reputational damage, and legal consequences, which can have detrimental effects on the survival and growth of SEs (SecurDI, 2023).

The level of awareness of information systems security remains low yet it plays a critical role in small enterprise management in Uganda, as it deals with the confidentiality, privacy, integrity, and availability of data and information which is one of their most valuable resources. Generally, SEs have been seen as a weak spot in information security and cybersecurity management, which is mainly due to their size and lack of corporate information security policies (Mário Antunes, 2021).

The National Cybersecurity Strategy report (Guidance, 2022) posits information security as a big challenge in Uganda with a remarkable increase in cybercrime ripping off the country millions of money which negatively affects the economy. The 2023 cybercrime report by the Uganda Police acknowledged 245 cases of cybercrimes, marking a 14.3% decrease from the 286 cases reported in 2022 and these led to a loss of **$** 414,362, of which 24.46 % (**$** 101,340) was recovered (FIA, 2024). The two major categories of cybercrimes attributed to the loss were electronic fraud and obtaining money by false pretense. The report also notes that cybersecurity threats pose a serious risk to the integrity of the e- services and internet in Uganda (Guidance, 2022).

A survey done by the Government of Uganda pinpoint end-users as the weakest link in the cybersecurity chain which is attributed to lack of training imperative in taking informed security decisions when carrying out digital activities. More Ugandans are adopting digital technology and these need to be supported to develop a cybersecurity culture aimed at addressing the avalanche of security threats. Concerted cybersecurity capacity building activities play a vital role in reducing cyber risks and the digital divide (Guidance, 2022).

The government of Uganda does not have any arrangements for formal training in information security, and this is not yet adopted in any of the national education curriculums. Some private firms have made strides in offering specialized training to their employees and these are usually sponsored by the respective enterprises through in-house training or through third party training arrangements. The need for a more formal cybersecurity training programme in Uganda is more than ever if the users of digital technology are to cope with the ever-increasing cyber security threats. Small Enterprises in particular need to be better positioned to address information security threats by equipping themselves with skills encompassing both online and offline responses such as the knowhow on policy and compliance, physical environmental protection, risk assessment, access controls, incident management, monitoring, backup, malware identification and technical intrusions (Guidance, 2022).

1.3 Problem Statement

Information security threats among small enterprises in Uganda are more than ever yet these enterprises lack the tailored tools and frameworks needed to protect their information systems effectively. National information security guidelines and existing frameworks focus on large enterprises, making them impractical for resource-constrained small businesses (Alshboul & Streff, 2015). Consequently, many Ugandan SEs operate with minimal formal security measures, leaving a critical gap in their defense against cyber risks (NITA-U, 2022). This gap is evidenced by the rise of digital fraud, ransomware attacks, phishing, and other malicious attempts targeting small business to exploit their weak controls and low information security awareness (Otucu, 2024). The integrity, confidentiality, and availability of vital business data in small enterprises are therefore under threat, undermining their trustworthiness and sustainability in the digital economy.

It is in this context that the study proposed the design of an information security artifact to fill the identified gap guided by the Design Science Research (DSR) paradigm to iteratively design and rigorously validate a customized information systems security framework for small enterprises Uganda.

1.4 Research Objectives

1.4.1 Main Objective

The objective of the study was to design a framework for enhancing information systems security tailored to the specific needs of SEs in Uganda.

1.4.2 Specific Objectives

1. To analyze existing information security frameworks and standards and determine the requirements for an effective security framework suitable for small enterprises in Uganda.
2. To design a framework for enhancing information systems security among SEs and the structure needed to protect internal data against information threats and vulnerabilities.
3. To validate the designed framework.

1.5 Research Questions

1. What are the requirements for establishing an effective information systems security framework for SEs in Uganda?

2. How are the existing information security frameworks addressing the information systems security needs of the SEs?
3. How can a framework for enhancing information systems security among SEs be designed and validated?

1.6 Deliverables and Outcomes

The main deliverable of the study was a framework for enhancing information systems security among small enterprises that was to be validated and adjusted based on information gathered from IT professionals, managers, and system end-users from within the sampled SEs. The proposed framework was to form a benchmark for small enterprises to enhance the security of their information systems.

1.7 Scope of Research

The research was conducted on information security frameworks among Small Enterprises in the districts of Wakiso and Kampala, Uganda.

1.8 Significance of Research

The aim of the research was to develop a tool for enhancing information systems security among Small Enterprises (SEs) in Uganda. The proposed customized framework was meant to bolster the information security capabilities of SEs, hence improve their operational resilience and long-term sustainability. By equipping Small Enterprises with essential tools to enhance the confidentiality, integrity, and availability of their information assets, the framework facilitates the establishment of trust with customers and stakeholders, while ensuring compliance with regulatory requirements. Furthermore, the insights derived from this study may provide valuable knowledge to policymakers and industry bodies regarding the specific needs of SEs, thereby fostering the development of more supportive regulations and initiatives.

CHAPTER TWO
LITERATURE REVIEW

2.1 Introduction

This chapter addresses the pressing need for adaptable and effective information security measures tailored to SEs. The chapter provides insights into the state of art information systems security basics that are relevant to understanding the concept of information security frameworks among SEs. The section also contextualizes the existing theories and research pertaining to information security frameworks. The chapter is pivotal to this study since it gives insights into information security best practices which are very crucial in supporting day to day operations of SEs in Uganda. This chapter was very crucial in addressing the first two research questions on the requirements for establishing an effective information systems security framework for SEs in Uganda as well as the efficacy of the existing information security frameworks in addressing the information systems security needs of the SEs. Thorough understanding of the SEs under the scope of the study was critical in finding answers to these questions.

2.2 Information Systems

According to (Zwass, 2025) an information system is "a set of interrelated components for collecting, storing, and processing data and for providing feedback aimed at achieving the business goals". Information systems are used in various ways such as but are not limited to carrying out daily business operations, gaining a competitive advantage in the marketplace, interaction with customers and suppliers. Information systems dictate how a business carries out its daily operations in order to survive amidst the ever-evolving digital technology. The integrated components also provide a feedback mechanism that help enterprises achieve increased profits, better customer service experience and support decision making based on data statistics (Zemmouchi-Ghomari, 2021).

2.2.1 Information Systems Components

An information system has four major components and these include technology, people, processes and data (Roch, et al., 2022). The section below provides more details on the information systems components.

I. Technology

Technology is the application of scientific knowledge to solve real-world problems. From the invention of the wheel to electricity and computers, technology is today an integral part of daily

life. In information systems, technology consists of hardware, software, and networks (Roch, et al., 2022).

- **Hardware:** Hardware are physical computing devices and these include routers, switches, computers, hard disks, keyboards, iPads, among others (Mukherjee, 2022). Hardware powers the capabilities of other components such as software, data and telecommunication by providing an interface on which they can run. Without hardware, it is difficult to realize the importance of these other components. Systems such as customer relationships management systems, transaction processing systems, management information systems can run simultaneously on a single hardware server computer. Advancement in technology has introduced new dynamics where hardware is being provided as a service. These services include server as a service (SaaS), infrastructure as a service (IaaS) among others (Mukherjee, 2022).
- **Software:** Software is simply a set of instructions, data or programs that can operate computers and execute specific tasks (Hashemi-Pour, 2024). Software is a variable part of a computer that defines applications, scripts and programs that run on a device (Hashemi-Pour, 2024). Software has two categories, i.e., application software and system software. System software is an operating system that is installed on hardware and is used to manage that hardware. System software provides a platform on which other applications can run. Application software is meant to perform particular tasks as requested by users (Zwass, 2025). Just like software, hardware is useless without software.
- **Networks:** Networks connect computer systems in order to convey information. Wired or wireless modes such as fiber cables, microwave radios, radio waves can be used to establish a communication link (Zwass, 2025).

II. Data

Data may be discrete or continuous values used to convey information. Data is useless in its raw form and hence has to be transformed to make informed business decisions. All businesses rely on data for business operations. Data is a very powerful tool in projecting sales, discovering new markets, analyzing market trends among others (Mukherjee, 2022).

III. People

Humans are a vital component of any information system. These may be comprised of technical personnel such as system administrators, business analysts, systems analysts' software developers

and non-technical human resources such as employees who use information systems to perform their business roles. All must be trained to efficiently use the information systems (Zwass, 2025) .

IV. Processes

Processes form the sequence of activities that businesses undertake to realize specific objectives. Information systems are increasingly being ingrained into these processes, rendering operations more efficient and controlled. Mere automation of tasks is not sufficient; companies need to apply information systems in a strategic manner to enhance both internal operations and external relationships with suppliers and customers (Roch, et al., 2022).

2.2.2 Types of Information Systems

Most companies have systems that support daily business operations. These systems can be used at strategic, operational and tactical levels. Information systems are categorized into transaction processing systems, management information systems, decision support systems, and executive support systems depending on the level at which they are applied. These systems provide up to date information that is vital in making business decisions and achieving the business goals (Zemmouchi-Ghomari, 2021). Below is a breakdown of the different types of information systems.

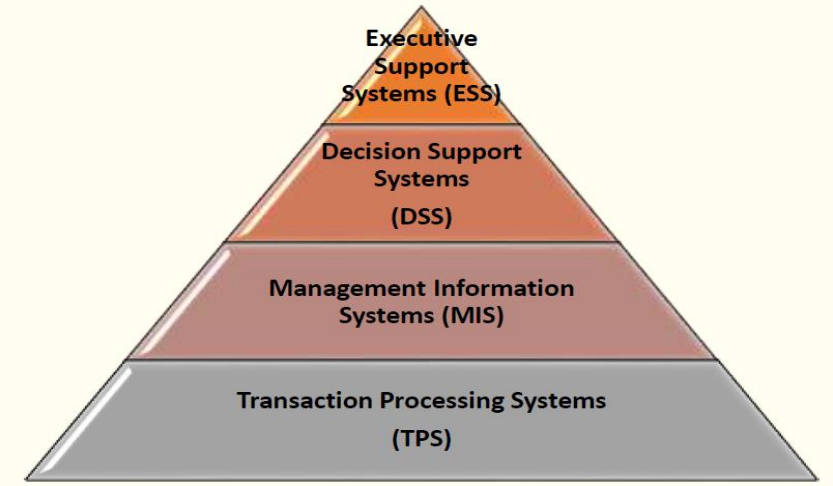


Figure 4:1: Information System Types

Source (Zemmouchi-Ghomari, 2021)

I. Transaction processing system (TPS)

TPS is used by businesses to perform daily routines such as processing payrolls, keeping employee records, general ledgers for accounting among others. Transaction processing system is used by

teams at the tactical level within a business to carry out the daily roles. Different levels of access rights can be defined within the TPS for clear segregation of duties (Zemmouchi-Ghomari, 2021).

II. Management Information Systems (MIS)

MIS are designed to support management of an enterprise with oversight, decision making, administration and control. The data obtained from the TPS and that from external sources such as websites and newspapers feed into the management information systems that summarize and give an overview of essential business operations (Zwass, 2025).

III. Decision Support Systems (DSS)

Decision support systems are designed to aid in decision making within a business. More and more businesses are increasingly depending on data for critical business decisions and this has triggered a DSS that can perform business data analytics. Decision support systems can be model-driven or data-driven. The model-driven decision support system is preprogrammed and can be applied to a selected dataset that is relatively small to form a basis for decision making. The model might be applied to sales of a certain month in order to determine the selling price in the following month. The data-driven DSS analyzes large volumes of data spanning over long periods of time. Data-driven DSS can perform business intelligence analysis by mining data from different sources which support decision making at strategic levels within the business (Zwass, 2025).

IV. Executive Support System (ESS)

ESS provide data in a more condensed form. These data can be presented in visuals such as digital dashboards for senior managers to easily drill through and make decisions. ESS tracks critical data such as competitor data, new taxes which can be used by top management in making decisions that require assessment and holistic view of the business performance. Data from MIS and DSS is aggregated into the executive support system (Zemmouchi-Ghomari, 2021).

2.3 Information Security

Information security is extremely important in protecting an organization's data from threats, maintaining business continuity, minimizing potential losses and enhancing return on investment and chances. The increasing reliance of small enterprises on information technology (IT) to carry out their operations more efficiently calls for tougher information security measures.

(IBM, 2024) defines information security as the safeguarding of crucial information against unauthorized access, alteration, exposure, use, or dislocation. The goal of information security is to protect the enterprise's information by reducing the threat of loss of confidentiality, integrity, and availability of that information to an acceptable level. It is vital for an enterprise to adopt an information security programme. According to (Committee, n.d.), an information security programme contains two major segments: risk analysis and risk management. The risk analysis phase is concerned with inventory of all information systems such as TPS, CRM, ERP, DSS which are categorized according to the value each system has on the business, as well as its vulnerability to cyber threats. Risk management entails selecting the controls and security measures that are aimed at reducing the organization's exposure to risk to an acceptable level. It is crucial for an organization to adopt a risk management plan as part of the information security framework where information security measures are complemented by controls such as computer, administrative, personnel and physical security (Committee, n.d.).

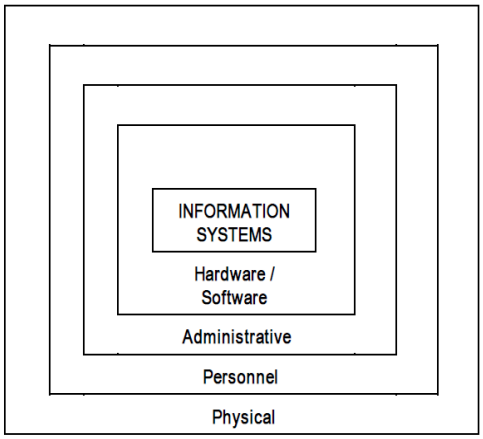


Figure 4:2 Complementary Layers of Information Security

Source: (Committee, n.d.)

2.3.1 Main Elements of Information Security

Information security protects sensitive information from unauthorized activities, including inspection, modification, recording, and any disruption or destruction. The goal is to ensure the safety and privacy of critical data such as customer account details, financial data or intellectual property. The basic tenets of information security are confidentiality, integrity and availability. Every element of the information security program must be designed to implement one or more of these principles (Imperva, n.d.). Below are the main elements of information security.

- Confidentiality: Confidentiality ensures that information is only accessible to authorized users. Measures should be put in place to prevent unauthorized disclosure of information. Personal information should be kept private and should only be visible and accessible only to those individuals who own it or need it to perform their business roles.
- Integrity: Integrity ensures that data is consistent over time and that unauthorized changes are prevented (additions, deletions, alterations). Data must be accurate and reliable and should not be modified incorrectly, whether accidentally or maliciously.
- Availability: Availability aims at making software systems and data fully available when needed (or at a specified time). The IT infrastructure, the applications and the data must be available when they are needed for business operations or for its customers.

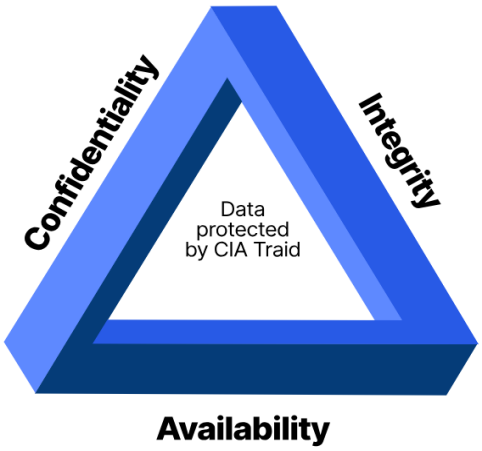


Figure 4:3: CIA Triad

Source: (Imperva, n.d.)

2.3.2 Information Systems Security

Many businesses are depending on information systems to execute their daily business operations. This dependence on information systems has attracted cyber-attacks for monetary gains and competition for customers. Once information is exposed, there is loss of confidentiality, and the original data may be altered to suit the attacker's needs. The information systems may also be made unavailable to the intended user through denial-of-service attacks. Businesses should put in place controls to ensure the security of their information systems (Zemmouchi-Ghomari, 2021).

2.3.3 Information Systems Security Key Success Factors

Information systems security is a concern of all businesses in today's digital era. The increasing reliance of businesses on technology to facilitate their daily business operations has triggered information security threats such as malware, phishing emails, rogue devices, malicious insiders among others (Limited, 2020). Many businesses have put control measures in place such as firewalls, antivirus, security policies to manage the threats. Despite these controls enterprises and particularly small enterprises in Uganda continue to face the security threats, vulnerabilities and risks (Arbanas & Hrustek, 2019). This should act as a trigger for business to identify and understand the information systems' key success factors. A study by (Arbanas & Hrustek, 2019) recognizes information security policy, management support and security training and awareness as the top three key success factors of information security.

I. Information Security Policy

The information security policy provides clarity on the guidelines, procedures, rules, expectations or approach an enterprise can take to enforce confidentiality, integrity and availability of information systems. Security policies span from high-level documents that align to the business' goals and objectives to low-level security policies that address the enterprise' specific issues. The security policy defines the overall security strategy and can be used in conjunction with other standardized documents such as standard operating procedures to achieve the security goal of the company (Grimmick, 2024). The security policy specifies the roles and responsibilities of each individual in the enterprise and should be clear, specific, concise and aligned to the organization's goals (Arbanas & Hrustek, 2019). Compliance with the security policy encourages an effective security culture where employees understand every detail of the policy and are aware of their roles and responsibilities in the enforcement process (Arbanas & Hrustek, 2019). Security policies can be program specific, issue specific or system specific. Program specific policies are strategic blueprints that provide guidance on the purpose, scope and onus of users in the security program. Issue-specific policies address more specific issues such as user acceptance policy, social media policy, and bring your own device (BYOD). System specific policies focus on particular systems such as firewalls, servers and enterprise resource planning (ERP) (Grimmick, 2024). For an information security policy to be effective, it should have a clear purpose for which it is drafted, a properly defined scope, commitment from senior management, tailored to business' risk appetite among others (Grimmick, 2024).

II. Management Support

Several research point to management support as an important factor in cultivating an effective information security culture. At a strategic level, management implements budgets aimed at financing information security activities such as awareness and training, human resources such as information security experts and IT equipment used in enforcing security controls. Management's support for information security also creates an environment where all employees are obliged to be compliant with the security policy. Management's reluctance to support information systems security would eventually trickle down to employees due to absence of a strategic direction on information security and would further expose such systems to security threats (Arbanas & Hrustek, 2019).

III. Information Security Training and Awareness

Security policies should be shared with staff and training sessions arranged for all employees. Training sessions can be virtual or physical and these can cover security procedures, data protection measures, access protection measures, and sensitive data classification. Employees come from different backgrounds and maybe naive of information systems security threats, risks and vulnerabilities. Such training brings employees up to speed with the existing risks and how to address them. Through such training, employees gain an understanding of their roles and responsibilities in enforcing the information systems security program (Arbanas & Hrustek, 2019).

2.3.4 Risk Analysis

Risk assessment in information security revolves around the identification, estimation, and acceptance of core security methods to minimize the risk associated with security weaknesses. Using risk analysis, an organization can evaluate its systems from the attacker's perspective which provides a much more complete understanding of likely threats to an organization (Blackduck, n.d.). The risk analysis model has four steps.

- **Identification:** The identification phase requires identifying all significant assets that an organization possesses, in terms of both hardware and software, and building a risk profile for any sensitive data that is produced, stored, or transmitted by these assets.
- **Assessment**. Once the security risks associated with critical assets are identified, an assessment is undertaken to determine how best the organization can spend time and resources to mitigate the risk.

- **Mitigation**. This phase involves finding possible solutions and implementing security measures for every risk identified during the assessment.
- **Prevention**. The prevention phase identifies tools and processes which can be implemented to minimize threats and vulnerabilities from occurring within the organization.

2.3.5 Risk Management

Risk management is defined as "The process by which an organization deals with risk" including assessing risk and developing strategies to manage risk. (McGrath & Jonker, 2025). Business risks can arise from a number of things, such as but not limited to financial exposure, regulatory obligations, applications of technology, governance failures, accidents, and natural hazards (McGrath & Jonker, 2025). The ISRM process is a detailed one and has the following stages (Rapid7, 2024).

Risk Identification: Risk identification entails identifying an asset, vulnerability, threat, and mitigative strategy. The confidentiality, integrity, and availability of assets with the most significant impact to the organization is assessed to ensure they are not compromised. Furthermore, deficiencies in the organizational processes resulting in the threats are considered and the controls taken to mitigate these weaknesses are determined.

- **Information security risk assessments:** The information gathered about assets, vulnerabilities, and controls is used in assessing risk. *Risk = (threat x vulnerability (exploit likelihood x exploit impact) x asset value) - security controls*.
- **Risk management strategy:** The enterprise can view and analyze a risk and decide the appropriate treatment i.e. remediate, mitigate, transfer, accept the risk, or avoid the risk.
- **Risk communication strategy:** Any treatment selected should be communicated throughout the organization. Stakeholders should know the price of attending to or ignoring a risk and have a sound rationale for their final decision. Roles and responsibilities should be clearly defined with specific accountability embedded into individuals and teams for engagement in the process
- **Rinse and repeat:** This is an ongoing process. If the treatment plan that requires implementing a control is chosen, that control needs to be continuously monitored.

2.4 Information Security Frameworks and Related Works

This section highlights some of the popular frameworks and the previous research carried out by scholars in information security frameworks. The knowledge gained from this section was very important in devising a conceptual framework for small enterprises in Uganda based on the research objectives.

I. National Information Security Framework

In 2014 NITA-U developed the National Information Security Framework (NISF) that was to serve as a conceptual structure for guiding information security activities in the country. The framework comprised of elements required to manage a functional area such as information, personnel and physical security. The framework guidelines devised a common approach that was meant to address internal and external information security. A multi-layered structure detailing mandatory security activities, roles, responsibilities and their relationships aimed at securing information and other assets that support the government in conducting its operations was adopted which was to apply to all stakeholders irrespective of their functions. The US ISO/IEC 27001 Plan-Do-Check-Act (PDCA) model was targeted for continuous improvement within the security programme.

Figure 4:4: Security Governance and the PDCA Model

Source: (NITA-U, 2014)

The NISF is a risk-management driven framework that holds accounting officers responsible for implementation of security measures to address information security threats. (NITA-U, 2014). However, the framework focused on information security outcomes rather than activities and requires one to comprehend information security roles and responsibilities that play a vital role in

empowering humans and institutions on information security capacity building (NITA-U, 2014). These are very good strides in enhancing information security among institutions but are highly focused on technical systems and established institutions leaving small enterprises out of the loop.

II. ISO/IEC 27001

The International Organization for Standardization 27001 (ISO 27001) standard provides requirements for establishing, implementing, maintaining, and improving an information security management system (ISMS). "An ISMS is a systematic approach to managing the confidentiality, integrity, and availability of information assets". The framework explores all the core aspects of information security such as risk assessment, monitoring, auditing and development of information security policies. It lays out a set of controls that can be implemented by enterprises based on their unique needs and risks (community, n.d.).

The ISO 27001 details a risk assessment approach that follows PDCA (Plan-Do-Check-Act) model (Al-esaiy & Al-Shaibany, 2021).

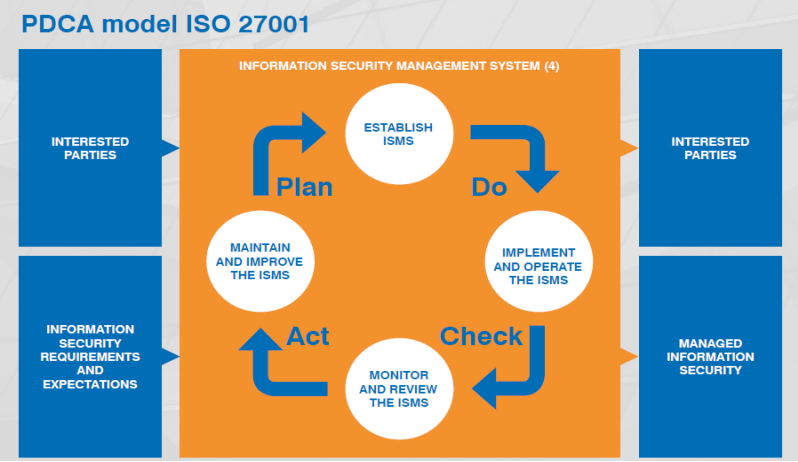


Figure 4:5: Plan-Do-Check-Act (PDCA) cycle

Source: (nqa, n.d.)

The Plan-Do-Check-Act (PDCA) cycle encourages continuous improvement of both people and processes.

According to (Mirtsch, et al., 2021), there is low adoption of ISO/IEC 27001 among small enterprises, and this is attributed to high costs involved in the implementation of the framework, lack of evidence on benefits outweighing the costs as well as quantifying the benefits of adopting ISO/IEC 27001.

III. The Center for Internet Security (CIS)

The CIS framework guides on the procedures for identifying, developing, validating, and sustaining best practices for a healthy information security programme. Critical Security Controls are based on real world attacks and threats which are updated from time to time to address changes in the threat landscape. Controls ranging from essential information security practices to advanced threat detection and prevention are documented in the framework (Moffat, n.d.). The CIS security controls are divided into three categories:

a) Basic Controls: These guide on continuous practices which should be undertaken by an enterprise to maintain its information security health. These form the first segment that covers six controls (1-6).
    1) Inventory and control of enterprise assets
    2) Inventory and control of software assets
    3) Data protection
    4) Secure configuration of enterprise assets and software
    5) Account management
    6) Access control management
b) Foundational Controls are more technical compared to basic controls and involve more specific measures. They sharpen the technical defenses, and these include the controls from (7-16).
    7) Continuous vulnerability management
    8) Audit log management
    9) Email and web browser protections
    10) Malware defenses
    11) Data recovery
    12) Network infrastructure management
    13) Network monitoring and defense
    14) Security awareness and skills training
    15) Service provider management
    16) Application software security

c) Organizational Controls form the last segment of controls (17-18) which focus on the strategic implementation of information security with the intent of creating a culture of information security within the business.

17) Incident response management

18) Penetration testing

CIS Critical Security Controls provides guidelines for implementing technical security and operational controls which can be adopted by any enterprise (Kirvan, 2023). The CIS framework has also demonstrated the need for customizing an information security framework to suit the needs of a particular organization as well as defining the three implementation groups which leverage organizations to choose a group that suits their business strategy. However, the framework does not address risk analysis or risk management but is rather focused on reducing risk and strengthening technical infrastructures (Kirvan, 2023).

IV. The NIST Cybersecurity Framework (CSF)

The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) was developed by the US government in collaboration with the private sector. Different stakeholders were engaged in the development cycle to ensure that the unique needs were captured. Paying attention to detail has made the framework one of the most widely adopted and recognized security frameworks in use. Features such as flexibility, scalability, and adaptability have made the framework a suitable choice for enterprises of all sizes. The framework consists of five core functions i.e., Identify, Protect, Detect, Respond, and Recover with each function consisting of a set of outcomes, activities, and subcategories which enterprises can use to define and set their information security goals as well as actions. The implementation tiers and profiles included in the framework help enterprises to align information security practices with their risk appetite, resources, and objectives (Technology, 2024).

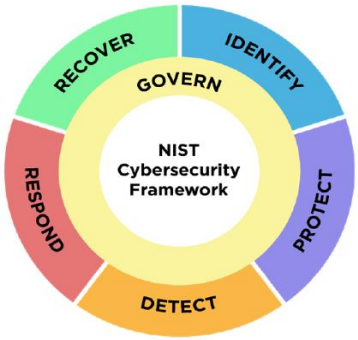


Figure 4:6: CSF Functions

Source: (Technology, 2024)

Recognizing the importance of small enterprises in the economy, Richard Kissel authored the NIST Interagency Report (NISTIR) 7621 specifically targeting information security of small businesses. NIST Interagency Report (NISTIR) is a guiding document on how small businesses can best protect their information, systems, and networks (Paulsen & Toth, 2016). According to NISTIR 7621, three major areas, i.e., essential information security practices, highly recommended practices, and other planning considerations can be addressed by small businesses. The standard assumes essential practices (specific actions) which can be taken by small enterprises since they do not have the required resources to perform certain functions. To sum it up, the NISTIR 7621 standard lists specific security controls that should be implemented by small enterprises since these may lack the required IT skills (Alshboul & Streff, 2015). The essential practices are summarized in the table below.

Table 4:1: NIST 7621 Essential Practices

Source: (Alshboul & Streff, 2015)

Antivirus
Internet Security
Firewall
Patching
Backups
Physical Security
Wireless Security
Employee Awareness
Individual User Accounts
Limiting Access

NISTIR 7621 did a great job in specifying the basic security practices that can be adopted by small enterprises to strengthen their information security posture. The standard provides insights into

technical practices such as ensuring operating systems are patched, firewalls are in place and properly configured, installing antivirus, data backups among others. These are great strides in ensuring information security, but from the strategic level small enterprises need to understand information security of their businesses and why it is important. Small enterprise owners and executives need to embrace information security and adopt a strategy to ensure information security best practices are in place. Small enterprises also highly depend on outsourced IT services and vendors due to limited budgets and lack of internal IT expertise, but NISTIR 7621 does not provide details on how to manage risks related to third party vendors. For an effective information security program, an information security strategy must be documented which does not come out clearly in the NISTIR 7621 standard.

V. A Framework to Enhance Information Security Governance in SEs

In their research, (Mwanje, et al., 2023) explored the challenges faced by Small and Medium-sized Enterprises (SMEs) in the Fort Portal Central Division as they sought to improve their information security. The challenges identified by the researchers included limited resources, budget limitations, and inadequate IT expertise in creating and enforcing security policies. Based on their findings, they proposed a framework where information security would be embedded into IT governance in small and medium enterprises. Their framework addressed the direct control cycle, that comprised of various management levels i.e., strategic, tactical, and technical (Manjezi & Botha, 2019). They also examined the necessary importance of the board and executive management in creating strategic direction that trickle down to operational levels. Their proposed framework included an Audit Function at the technical level in order to reduce the expert gap faced by SMEs due to the IT and security experts. The research emphasized that key components including Audit Function, Risk Assessment, Legal and Regulatory Compliance and Incident Handling are the vital for an effective information security program (Mwanje, et al., 2023).

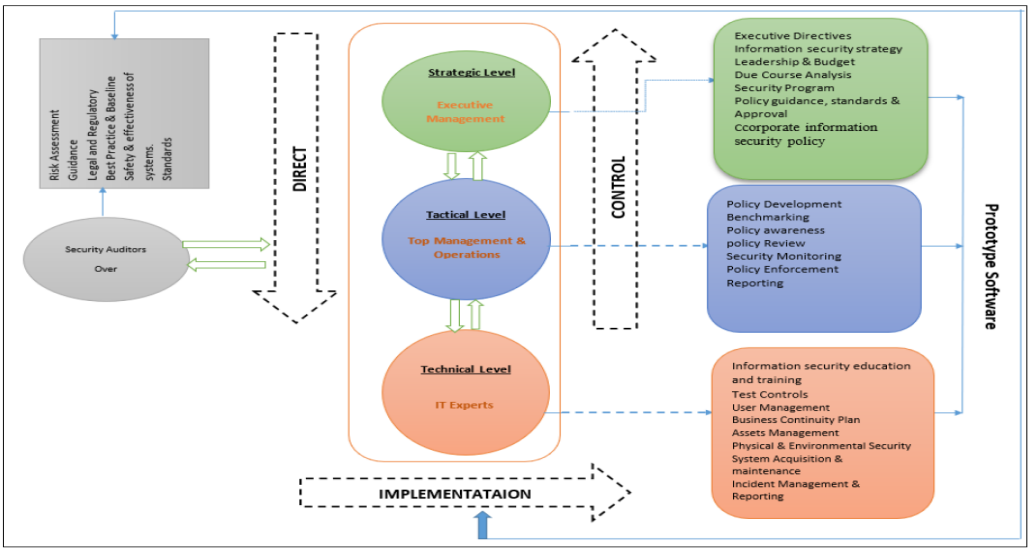


Figure 4:7: Framework for information Security Governance

Source: (Mwanje, et al., 2023)

The framework provides for information security policies and awareness at technical levels but does not provide details on the roles and responsibilities of end users (acceptance use policy). For a successful information security programme, the roles and responsibilities of end users must be clearly defined, and this must be backed up by management support. Most of the small enterprises outsource most or all of the IT activities but the framework doesn't guide on third party risk management which must be given due focus.

VI. A Proposed Best-practice Framework for Information Security Governance

Research carried out by (Gashgari, 2017) adopted three stages to accomplish three objectives in devising a framework for enhancing information security governance among enterprises i.e., forming the guidance, identifying the critical success factors (CSFs) and mapping the CSFs to the essential areas of information security governance. According to the research, information security must be integrated into corporate governance. It further states that a good information security programme delivers strategic alignment, risk management, resource management, performance measurement and value delivery. It is equally important to identify the critical success factors (CSFs) that facilitate improvement from a high level across the essential governance areas for effective governance as summarized in Table 2.2. The stages for the development of an effective information security framework are shown in figure 2.7.

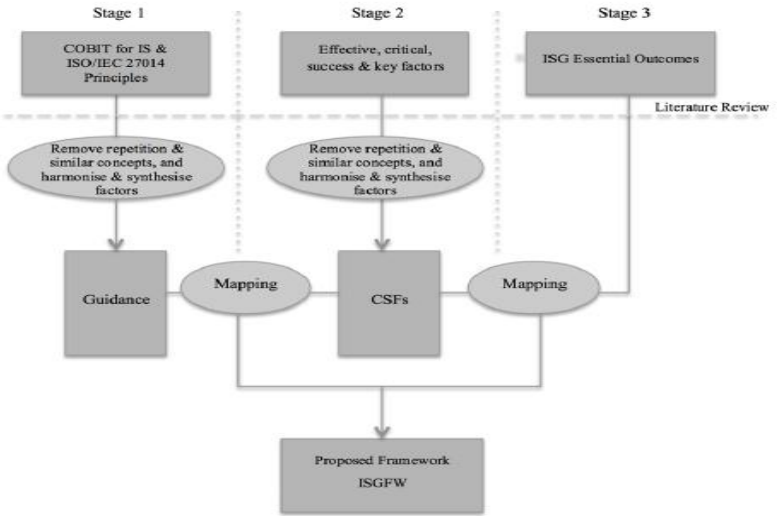


Figure 4:8: Stages in developing a framework

Source: (Gashgari, 2017)

The research posits that a properly implemented information security framework should provide five outcomes, i.e., strategic alignment, value delivery, performance measurement, risk management, and resource management. According to the framework, it is the responsibility of enterprise leaders to ensure that the five essential areas function successfully.

Table 4:2: Information Security Framework by Gashgari

Source: (Gashgari, 2017)

ISG Area	Guidance		CSF
Strategic Alignment	Consider IS as an organization wide issue	1	Integrate IS with business activities
		2	On-going strategic alignment
		3	Determine clear IS roles & responsibilities and be held accountable
	Act in professional and ethical manner	4	Visible involvement & leadership
	Conform & comply with internal & external IS requirements	5	Ensure IS policies and practices comply with law & regulations and relevant IS requirements
Performance Measurement	Provide timely & accurate information on IS performance	6	Ensure timely and transparent reporting of IS performance and issues
	Review IS performance in relation to business outcomes	7	Constant review of IS performance
	Promote continuous improvement in IS	8	Improve IS on an on-going basis
Value Delivery	Deliver quality & value to stakeholders	9	Effective communication
		10	Effective business continuity/disaster recovery plan
Risk Management	Adopt risk based approach	11	Determine risk appetite
	Evaluate current & future information threats	12	Ensure regular risk & threats assessment
	Protect classified information	13	Protect critical and sensitive assets
	Concentrate on critical business applications	14	Identify critical applications & information systems
	Develop systems securely	15	Integrate IS with systems development lifecycle
Resource Management	Foster an IS positive culture	16	Effective IS awareness and training
	Set the direction of investment decisions	17	Adequate investment & resource commitment of IS

The framework by Gashgari provides good steps in enhancing information security for enterprises, however this is a proposed framework which has not been validated to test its efficacy among small enterprises.

VII. Cybersecurity Guide for SEs: Protecting Small and Medium-Sized Enterprises in the Digital Era

In their research, "Protecting Small and Medium-Sized Enterprises in the Digital Era" (Liontos, et al., 2025) designed a Java-based tool aimed at evaluating cybersecurity among SMEs based on a list of predefined measures and policies. This tool was intended to evaluate the current cybersecurity posture among SMEs in order to identify areas for improvement. The researchers were guided by the most popular and recognized standards such as ISO/IEC 27001:2022, the NIST Cybersecurity Framework, and ISO/IEC 27701:2019 when coming up with the questions. The key areas of information security that were covered in the questionnaire include policy development, data protection and incident response. The tool consisted of 30 questions that was uploaded to GitHub repository for any SME to access and download (Liontos, et al., 2025). However, the tool designed is very technical and process oriented. Little is mentioned about the human factor in the questionnaire, which is a very important component of information systems. The aspect of risk management is also not addressed in the questionnaire yet for an information security programme to be effective, thorough risk assessment must be conducted.

VIII. Analyzing Information Security Model for Small-Medium Sized Businesses

(Yazan & Kevin, 2015) reviewed the National Institute of Standards and Technology (NIST) framework for security in small and medium-sized businesses and developed an information security framework using the PDCA phased approach and the prescriptive approach of NISTIR 7621. The framework was customized to small and medium sized businesses and emphasized a rigorous approach to risk management.

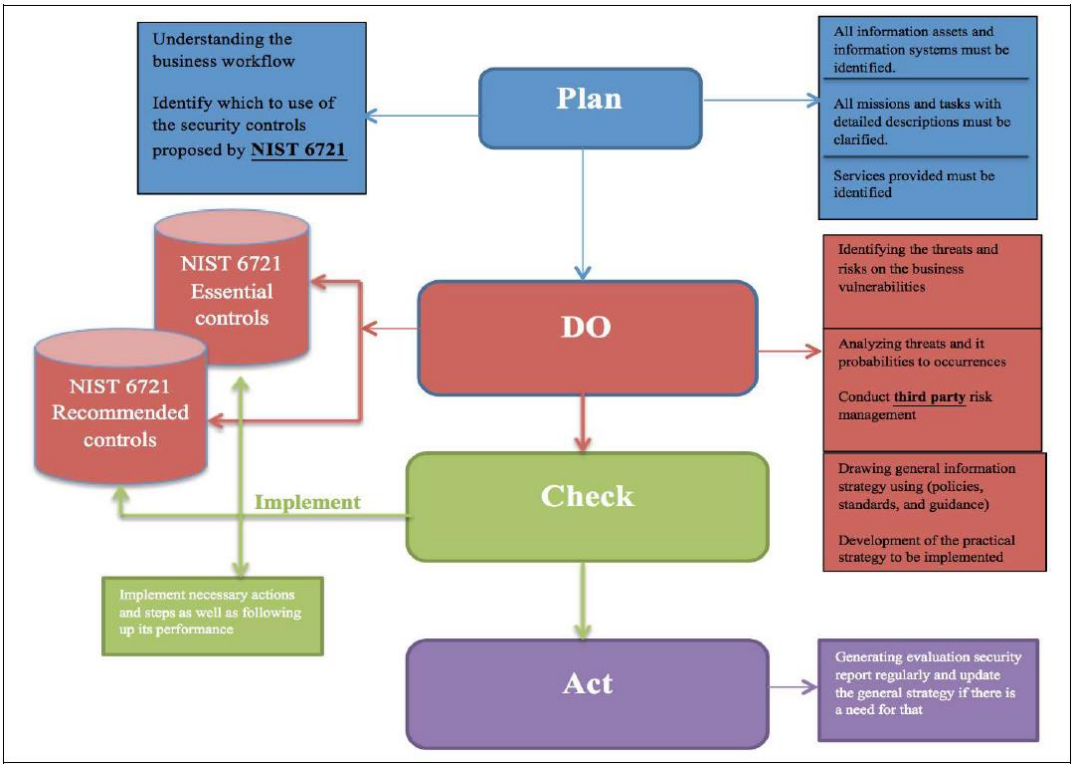


Figure 4:9: Security Model for Small-Medium Businesses

Source: (Alshboul & Streff, 2015)

The model was well designed to suit the security needs of small enterprises, but the feedback loop is very shallow. The act step only mentions a periodic security report and updating strategy as necessary. The model does not describe what metrics or audits initiate updates. Specifically, there is no mechanism for learning from security incidents.

IX. A Framework for Enhancing Systems Security

(Sharma & Sugumaran, 2011) designed a comprehensive framework aimed at enhancing information systems security by integrating technical, processes, and human factors across the entire information security program. The framework addressed information security from three core dimensions i.e. technology, processes and people. The technology aspect comprised of secure hardware, software, and network components. The processes laid down in the framework included security policies, procedures, and governance mechanisms. The people domain covered awareness, training, and role-based access controls.

The framework posits that security considerations should be embedded at all stages of the system development lifecycle (SDLC) right from requirements gathering to design, implementation,

testing, deployment, and maintenance. Further to this, the framework emphasized for continuous evaluation of threats, vulnerabilities, and impact to the organization as well as prioritizing possible mitigants. Clear, enforceable rules aligned with industry standards were included in the framework. In terms of access controls, the framework explored least-privilege principles, authentication mechanisms, and authorization processes. Quick wins on incident response, monitoring & auditing and security training aimed at bolstering the information security posture were highlighted in the framework (Sharma & Sugumaran, 2011).

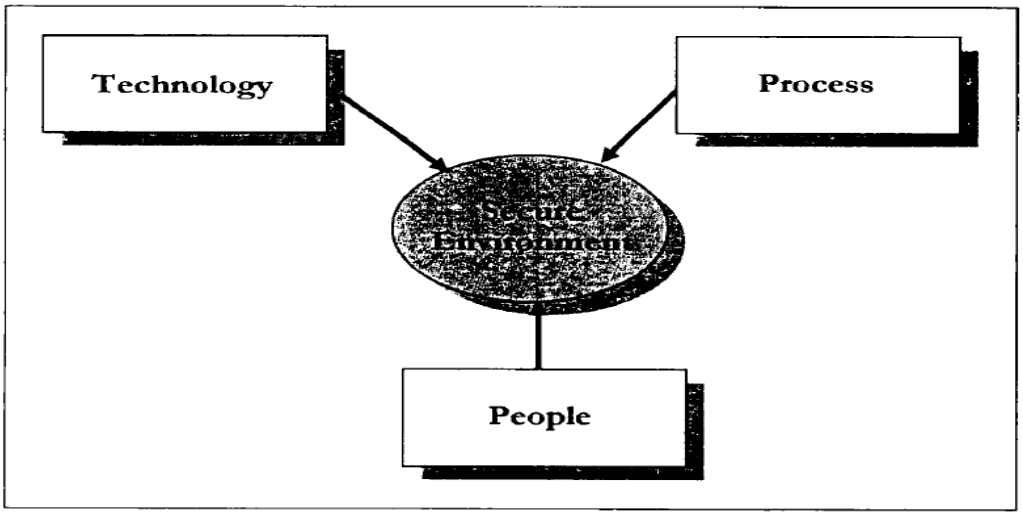


Figure 4:10: A Framework for Enhancing Systems Security

Source: (Sharma & Sugumaran, 2011)

2.5 State of Information Security among Small Enterprises in Uganda

Uganda's small enterprises (SEs) form the backbone of the economy (contributing about 20% of GDP in 2016) (Wanyama, 2017). Over the past decade, Small Enterprise adoption of digital technologies has grown, but information security practices have lagged. Many small businesses historically treated information security as a low priority "technical issue" rather than a strategic imperative (Wanyama, 2017). This section examines the state of information systems security among Ugandan small enterprises from focusing on security policies, security controls, risk management, and security awareness & training.

Security Policies in Small Enterprises

Prevalence of Policies: The majority of Ugandan small businesses have operated without formal IT security policies for most of the past decade. In the mid-2010s, few SMEs had documented

cybersecurity policies or plans in place. By 2022, a national IT survey found that 72.1% of businesses reported having no formal ICT policies at all (NITA-U, 2022). Dedicated information security policies are still rare with only about 0.5% of businesses having a standalone information security policy in place as of 2022 (NITA-U, 2022). The few enterprises that have policies have basic IT-related policies such as employee IT training policies (13.7%), acceptable use rules for company IT resources (around 13%), and general IT strategy/master plans (about 12%) (NITA-U, 2022). Policies for sensitive areas like disaster recovery/business continuity were reported by only ~3% of businesses (NITA-U, 2022), indicating that very few small firms have formal plans to handle major incidents. Overall, the data shows that documented cybersecurity policies have been the exception rather than the norm in Uganda's small enterprise sector.

Enforcement and Effectiveness: The lack of formal policies implies that enforcement mechanisms are often informal or absent. Without written policies, small businesses have tended to address security on an ad-hoc basis. Even among those with IT policies, enforcement is weak due to limited oversight and expertise. For example, one study noted that many enterprises continued to view cybersecurity "as a tech issue, not a business imperative," leading to poor top-down support for policy compliance (Wanyama, 2017). As a result, policy effectiveness has been limited, and the low uptake of policies correlates with persistent vulnerabilities and incidents. The Ugandan government has introduced laws like the Data Protection and Privacy Act (2019) and national cybersecurity frameworks, but small businesses have been slow in complying due to resource constraints and low awareness. In a nutshell, the prevalence of documented IT security policies among Uganda's SEs remains very low, and effective enforcement of cybersecurity rules is still generally lacking across the sector (NITA-U, 2022).

Technical and Procedural Security Controls

Adoption of Controls: Small enterprises have gradually implemented some basic security controls over the past decade, though advanced measures are still uncommon. A 2017 capacity-building workshop for Ugandan SMEs by NITA-U underscored that many businesses lacked even fundamental controls such as malware protection (antivirus), access controls, patch management, secure configuration, and firewalls (Wanyama, 2017). However, the 2022 survey data showed improved uptake of basic technical controls such as antivirus software which is the most widely used protection among businesses. Network firewalls and regular data backups have also gained

some traction though still low. Other controls such as intrusion detection systems, encryption for sensitive data, security patches/updates remain less prevalent (NITA-U, 2022).

The last decade has shown a slow improvement in basic cyber defenses among Ugandan SEs. Most small firms still operate with a minimal security stack. Many rely on consumer-grade anti-malware and built-in firewalls and lack layered defenses. For example, the majority have no formal intrusion monitoring, no encryption of devices, and no multi-factor authentication for users (NITA-U, 2022). This means that while basic controls are more common now than a decade ago, SEs' networks remain relatively easy targets for cyber threats. Inadequate maintenance of controls further undermines their effectiveness. According to (Fulbright, 2020) over 80% of successful attacks on firms stem from poor "cyber hygiene" such as unpatched systems and weak passwords). In Uganda, this pattern holds true, small businesses that do implement controls often fail to update or audit them regularly. In summary, technical security measures in SEs have improved modestly (especially anti-virus and backup practices), but many critical controls are still absent or not rigorously maintained, keeping the overall security posture weak.

Risk Management Practices

Formal information security risk management is largely absent in Uganda's small enterprise sector. Most SEs do not conduct systematic risk assessments to identify threats and vulnerabilities in their IT environments (Wanyama, 2017). Instead, they tend to have a reactive approach, addressing issues only after incidents occur. Surveys and studies consistently show a low perception of risk among small business owners. In 2022, over 58% of businesses said they do not feel at risk of cybercrime (NITA-U, 2022). This complacency means many SEs have not taken steps to identify what their key information assets are or how they could be attacked. Even basic preventive practices like vulnerability scanning or risk audits are rare in the SE community. A 2018 cybersecurity assessment noted that Uganda had roughly 300 certified security professionals in total (Adomako, et al., 2018), signaling a severe skills shortage. Most small enterprises cannot afford dedicated cybersecurity staff or consultants, so ongoing risk assessment is simply not performed.

Because of the limited risk identification, proactive risk mitigation is equally weak. Few SEs have risk mitigation plans or budgets. Very few businesses have business continuity or incident response

plans. When cyber incidents occur, small businesses often handle them informally. The prevailing response to an incident is to "fix the problem internally*"* if possible and move on (NITA-U, 2022).

To sum it up, the risk management practices among Uganda's small enterprises remains immature and reactive. While larger organizations are adopting formal cybersecurity frameworks, SEs largely are not. Most enterprises have no dedicated risk management processes and rely on basic security measures (if any) and hope for the best, a strategy that leaves them vulnerable to ever-evolving cyber threats.

Security Awareness and Training

Employee security awareness in Uganda's small enterprises has generally been low, though there are signs of gradual improvement. Over the past decade, many small business employees had little or no training on digital security practices. A 2016 global survey highlighted that even IT managers often saw information security narrowly implying that non-IT staff are likely to be even less informed. Common risky behaviors (weak passwords, falling for phishing emails, etc.) have been widespread. Most small businesses do not conduct regular cybersecurity training for their staff (Wanyama, 2017).

For small enterprises, cyber awareness is often treated as an afterthought, not a continuous program and the consequence of this is ongoing vulnerability due to human error. According (Fulbright, 2020), inadequate user awareness and cyber-hygiene contribute to the majority of successful cyber-attacks. Therefore, continued efforts by government and partners are needed to ensure that regular training programs become a norm for small businesses, as an alert and informed workforce is often the best defense against cyber threats.

This section has explored some of the most popular and widely recognized frameworks as well as existing research on information security frameworks. A lot of research has been conducted in information security frameworks among small enterprises in both developed and developing countries. It is important to note that information security challenges faced by small enterprises in developing countries might not be the same challenges faced by small enterprises in developed countries. For instance small enterprises in USA employ between 100 to 1,500 employees and have turnover/ maximum sales of $40 million (Hait, 2021) while in Uganda small enterprises employee between 5 and 49 people and have total assets between UGX10 million but exceeding

100 million (UIA, n.d.). In the same spirit the unique challenges faced by small enterprises in the quest for information security solutions such as limited budgets, lack of internal IT expertise, overreliance on open-source software and third-party vendors among others might not be the same challenges faced by the small enterprises where the widely recognized standards for small enterprises such as NISTIR 7621 are developed and tested.

This study proposed a framework for enhancing information systems security tailored to the unique needs of small enterprises in Uganda by adopting the framework by (Yazan & Kevin, 2015) that was developed on the principles of NISTIR 7621 and ISO 27001. This study sought to employ a rigorous approach to risk management since many small enterprises in Uganda depend on open-source software as well as third party vendors for managing their information systems. Further to this, the study explored a top-down approach to information security emphasizing management's and business owners' commitment to improving information security posture in their respective enterprises.

2.6 Conceptual Framework for ISS among Small Enterprises

Ugandan small enterprises are confronted by information security threats as a result of limited resources, expertise, and customized guidance. Current security standards (national or international) are too generic, complicated, and expensive for SEs and thus leave them "out of the loop" while trying to apply advanced security controls (Yazan & Kevin, 2015). As a result, most SEs continue to be exposed to attackers such as data breach, fraud, phishing, ransomware among others. More than ever attackers are increasingly targeting the small enterprises since they do not have dedicated security resources, awareness, and procedures (Otucu, 2024). There is an evident necessity for a tailored framework to consider the distinct requirements and limitations of Ugandan SEs to enhance their security level without excessive complexity or expense.

The framework is grounded on (Sharma & Sugumaran, 2011) who designed a comprehensive framework aimed at enhancing information systems security by integrating technical, processes, and human factors across the entire information security program. The framework addressed information security from three core dimensions i.e. technology, processes and people. The technology aspect comprised of secure hardware, software, and network components. The

processes laid down in the framework included security policies, procedures, and governance mechanisms. The people domain covered awareness, training, and role-based access controls.

The framework posits that security considerations should be embedded at all stages of the system development lifecycle (SDLC) right from requirements gathering to design, implementation, testing, deployment, and maintenance. (Sharma & Sugumaran, 2011).

Drawing on these concepts, the suggested framework for Ugandan SEs was centered around people, process, and technology elements and mapped onto an iterative process methodology. Specifically, it was aligned with the Design Science Research (DSR) process, which consists of six main phases: problem identification, objective definition, artifact design/development, demonstration, evaluation, and communication. Integrating the people, process and technology dimensions with a DSR-based iterative process, the framework supports thorough coverage of security requirements and a continuous improvement cycle. It prioritizes solutions that are practical, straightforward, low-cost, and suitable for resource-constrained settings, which fits real-world circumstances in Uganda.

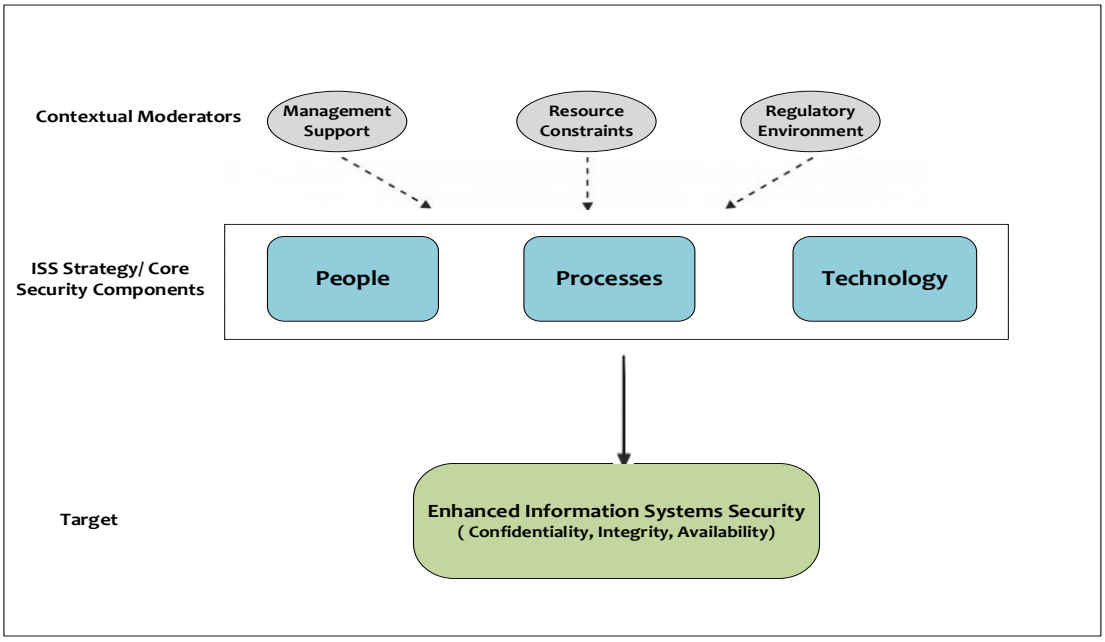


Figure 4:11: Conceptual framework for ISS

Source: Conceptualized by the researcher (2025)

The conceptual framework illustrates the proposed relationships. The independent variables (core security components) are shown in the middle all pointing toward the dependent outcome of

Enhanced Information Systems Security (CIA) at the bottom. The contextual moderating variables (management support, resource constraints, regulatory environment) are indicated separately (with dashed arrows), signifying that these factors strengthen or weaken the impact of the independent variables on the security outcome. In essence, strong management backing, sufficient resources, and the regulatory environment will amplify the effectiveness of people, processes and technology hence improving the confidentiality, integrity, and availability of information systems. The following sections explore each of the variables in detail.

2.6.1 Core Components of the Framework

The framework integrates clearly defined components that map to People, Process, and Technology dimensions. The three components address the security needs of SEs in concert and were the basis for the information security artifact to be designed and validated.

I. People Dimension

People are at the heart of information security. In small enterprises, this dimension focuses on cultivating a security-aware culture and building human capacity despite limited formal training. Key components include:

- **Security awareness and training**: (Whitman & Herbert J. Mattord, 2018) define training and awareness as "a managerial program designed to improve the security of information assets by providing targeted knowledge, skills, and guidance for an organization's employees". The study by (Gashgari, 2017) documented IS awareness as one of the critical success factors in ensuring the integrity, confidentiality and availability of information assets. Many of the information security breaches arise from human error. Therefore, conducting regular employee awareness training is vital in ensuring that all staff members are up to date on information security best practices as well as understanding their role in maintaining it. There is a great need for SEs to conduct training in phishing attacks, password management, safe internet practices among others (Leger, 2024). By fostering a culture of awareness, employees become an active part of the security strategy.
- **Management support and information security governance:** Leadership involvement is very vital in ensuring the security of information systems. SE owners and managers must lead security efforts, provide minimal resources, and mandate policies by example. Top-down dedication guarantees that security is not treated as "just an IT problem" and that

staff members take it seriously. Management should be engaged in a practical sense by approving security plans, attending training, and overseeing compliance.

- **Defined roles and responsibilities:** In small business, clear allocation of security responsibilities ensures accountability among staff. Roles can be split among different staff, one employee could be responsible for coordinating IT maintenance and backups, while another is responsible for access control and incident reporting. All staff must be equipped with information on how to report incidents.

People element interfaces with the remaining two aspects, i.e., process and technology by following and working on them. In the absence of educated and responsible people, the best tools and procedures will not work. Therefore, enhancing the human factor (through awareness, training, and leadership) increases the value of process controls and technology solutions.

II. Process Dimension

Process dimension covers policies, procedures, and structured activities that an organization uses to manage information security. The crucial practices tailored to SEs include:

- **Information security policy:** A study by (Bobbert & Mulder, 2015) on critical success factors suitable for business information security suggests that policy should be core a principle in information security governance if businesses are to safeguard themselves against the evolving cyber security threats. (Flowerday & Tuyikeze, 2016) posits that establishment of clear information security policies such as acceptance user policy, social media policy, bring your own device policy, information security policy among others are vital in ensuring the security of information assets. Such policies must be simple, clear, and relevant to the enterprise's business goals and compliant to regulatory standards.

- **Risk assessment and management:** A study by (Gashgari, 2017) on "A Proposed Best-practice Framework for Information Security Governance", lists risk management as one of the critical factors aimed at ensuring confidentiality, integrity and availability of information assets. The study emphasizes the need for thorough risk assessment to identify potential risks and their risk appetite. Given the meager sources, SEs can put in place a basic risk assessment process that involves periodically identifying the enterprise's vital information assets (e.g. customer records, financial data), the threats to those assets, and

existing vulnerabilities. A simplified risk register or checklist that tracks major risks can be put in place.

- **Incident response and recovery procedures:** The framework should have guidelines on how to respond to security incidents. These could be simple and concise steps to take such as measures to take if a computer is infected with malware or if a data breach is suspected. Data backup and recovery procedures are also essential for business continuity after an incident.

Process controls provide guidance on how individuals utilize technology. Policies and procedures codify the expectations: e.g., a policy might demand that all personnel utilize passcodes on their work equipment (people behavior) and have antivirus software installed (technology control). Conversely, compliance with processes such as periodic audits or incident drills yields feedback to enhance both the human and technical aspects of security. The process aspect thereby integrates the human and technical components into a workable program.

III. Technology Dimension

Technology consists of the tools and technical controls that protect information systems. In the SE context, the focus is on the determination of appropriate and affordable technologies that mitigate identified risks, without requiring large organizational budgets or special expertise. Important components include:

- **Security Controls:** According to (Flowerday & Tuyikeze, 2016) businesses must have security controls to ensure confidentiality, integrity and availability of information. A study by (Otero, 2015) further cements the importance of information security controls. The scholar urges that inadequacies in information security controls jeopardize information systems. The security controls include physical, technical and administrative controls that are implemented to facilitate integrity, confidentiality, and availability of information systems. Physical controls are procedures, measures and policies that focus on protecting non-digital assets and such include access cards, biometrics, lock keys, CCTV among others. Technical controls, also known as logical controls, are majorly software mechanisms such as firewalls, access control lists, network segmentation, intrusion detection/prevention systems which protect information systems. Administrative controls

also known as management controls put in place processes, procedures, policies for safeguarding information assets (Anwita, 2024).

- **Technical architecture and tools:** Where the business utilizes cloud services or third-party systems, technology decisions include choosing reputable providers with security certifications and activating their security features. For instance, an SE utilizing cloud email should utilize spam filtering and login notifications offered by the provider. Open-source tools can be utilized also (e.g., open-source VPN software for secure remote access, or free disk encryption tools for safeguarding sensitive information). The framework promotes multi-layered defense in simplified mode i.e. integrating endpoint protection, network protection, and data protection in layers. Every layer may not be the latest solution, but combined they increase the effort for an attacker to be successful.
- **Monitoring and logging**: Despite finite financial resources, (SEs) can embrace essential monitoring practices. This can include the periodic review of system logs, the setup of email alerts on particular events (such as repeated failed login attempts), or the use of free services that notify businesses when breaches relating to their emails have occurred.

The technological component provides the actual tools that enable or support information security, but it requires the support of people and processes. For instance, installing antivirus software is pointless if people do not pay attention to its alerts or if policy does not require updates. Technical solutions must be correctly configured and regularly maintained, which is itself a procedural activity, and used correctly by staff. In this framework, technology selection always balances against considerations like usability and affordability. Tools must be easy enough for the small enterprise staff to manage and preferably have little or no cost associated with them, otherwise, their viability will be compromised.

2.6.2 Enhanced Information Systems Security

Enhanced information systems security, i.e., confidentiality, integrity and availability, is achieved through an adequate information systems security strategy. A properly implemented strategy translates into the overall improvement in the small enterprises' ability to secure their information systems and protect their data from internal and external threats. There is a monotonic relationship between the information security strategy and improved information systems security. Properly

implemented technology, processes that are supported by people reinforce the confidentiality, integrity, and availability of information systems (Writer, 2024).

2.6.3 Contextual Moderators

The contextual factors can influence the effectiveness of an improved information systems structure and, consequently, the information security strategy. These factors can either facilitate or hinder the successful implementation of information systems security strategies. The intervening variables in this framework are:

- **Resource constraints:** According to (Gashgari, 2017), resource availability is an important factor in promoting a positive information security culture as well as setting the direction of investment decisions. The scarcity of financial, human, and technological resources can significantly impact the ability of SEs to implement security measures. For example, if a small enterprise lacks the budget to purchase advanced security tools or hire skilled IT staff, the overall security posture may be weak despite the adoption of security strategies. Conversely, sufficient resources can enable the acquisition of up-to-date tools and training for employees.
- **Management support:** Business owners and management should take a center stage in setting a tone for an information security focused culture (Ashmead, 2023). The commitment of small enterprise management to information systems security is crucial for a successful information security programme as it sends out a clear message to all employees that information security is an important aspect of the company's operations (Ashmead, 2023). If the management prioritizes security and allocates the necessary resources, the chances of successfully enhancing security are higher.
- **Regulatory environment:** Crucially the regulatory environment provides guidance that can moderate information security efforts. If the regulatory environment imposes requirements or incentives for cybersecurity (such as data protection laws or industry standards), it can enhance the effect of process improvements and technology adoption by compelling compliance. Conversely, a weak regulatory framework may not motivate small businesses to invest in security (Olsen, 2024).

The contextual factors serve as enablers or constraints that shape how effectively the People, Process, and Technology improvements translate into enhanced security outcomes. The dashed

arrows in the figure highlight that, for example, strong management support, sufficient resources, and a supportive regulatory climate will amplify the positive impact of the core security measures on the enterprise's security, whereas their absence could weaken it. Each moderator thus interacts with the independent variables' influence on security, underscoring the importance of considering the broader context in any small enterprise security framework.

CHAPTER THREE
RESEARCH METHODOLOGY

3.1 Introduction

This chapter presents the approaches employed in designing and evaluating the proposed framework for enhancing information systems security among small enterprises in Uganda by leveraging the industry best practices and adopting from the framework by (Sharma & Sugumaran, 2011)**.** The primary focus was to design a framework aimed at improving the information security posture among the enterprises in Uganda. The areas covered in this section include research design, description of study area, determination of sample size, sampling techniques, methods for data collection, data analysis and presentation.

3.2 Design Science Research method

The research was grounded on the Design Science Research (DSR) paradigm in Information Systems. The design science methodology is handy in creating artifacts, such as models, frameworks, or prototypes, that solve real-world problems and impart knowledge in a particular domain (Lazaar, 2024).

DSR is iterative and widely adopted in providing solutions to real-world problems and hence the most appropriate for this study's objective of designing an information security framework. In contrast to purely exploratory or explanatory research, DSR aims to design practical solutions and contribute knowledge through them. As it does so, it integrates rigor (by basing on theories that exist and employing systematic approaches) with relevance (by making sure the research is meeting a real-world requirement) (Baskerville, et al., 2018).

(J., et al., 2020) outlined the basic steps of the Design Science Research (DSR) process, which were adopted and rigorously followed in this study.

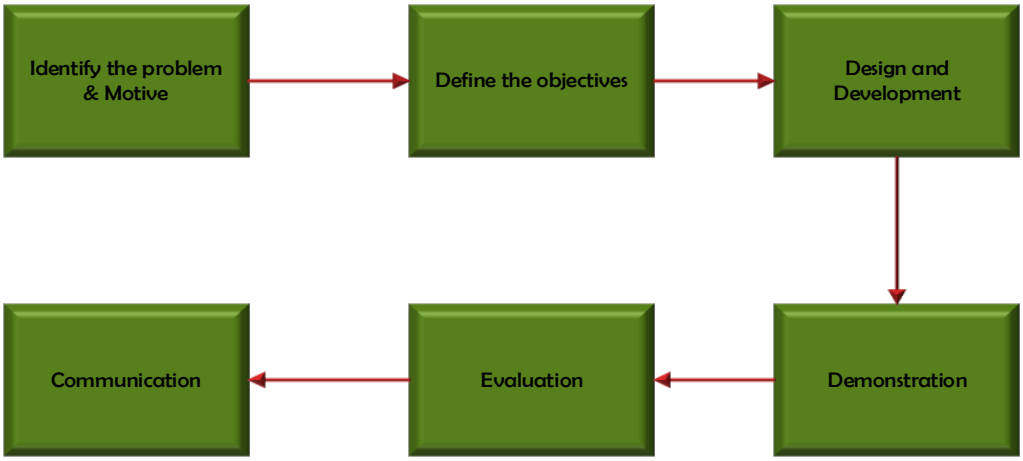


Figure 6:1: Design Science Research Process

1. **Problem Identification and Motivation:** Clearly identify the problem and justify the importance of a solution. For this study, the gap was the inadequate security of Uganda's small enterprise information systems due to absence of a tailored framework. The motivation was the pressing need to secure these enterprises against increasing cyber threats and ensure their sustainability. The researcher arrived at this problem through a comprehensive literature review and a preliminary needs survey with small business owners, which surfaced prevalent security challenges (such as absence of information security policies, weak controls) and agreement that available frameworks were not suiting their environment. This phase confirmed the significance of the research problem.
2. **Define the objectives:** Once the problem has been defined, define what needs to be accomplished. In this case, the objectives were to create a framework that is effective (enhances security outcomes for SEs), practical (possible to implement with few resources), and best practice aligned (drawing on proven security controls from standards but made accessible for SE use). These objectives were inferred from literature gaps and the target enterprises' specific requirements. Basically, the researcher converted general requirements (from research question 1 and 2) into design objectives for the artifact.
3. **Design and development of the artifact:** At this stage, the artifact which was a security framework that solves the problem and fulfills the objectives was created. Knowledge was pooled from literature on existing frameworks, standards, and existing research as well as the survey (empirical data gathered from Ugandan small businesses) to guide the design. Specifically, the design activity comprised: (a) Determining key components and framework

structure (adopting a phased approach of assessment, planning, implementation, monitoring inspired by both ISO 27001's Plan-Do-Check-Act cycle and NIST's recommended approach for small businesses); (b) Filling in each phase with detailed activities and controls applicable to the small enterprise environment and (c) Making the framework iterative and scalable (so that small businesses can improve continually and potentially include more sophisticated measures as they expand). The initial framework design was presented in Chapter 4, section on Framework Design, explaining how each component of the framework was derived (with sub-sections describing contributions from ISO 27001, NISTIR 7621, and empirical data). The design activity was iterative; the researcher returned to the framework components several times to refine them as more data arrived and as the framework was prepared for validation.

4. **Demonstration:** In the context of Design Science Research (DSR), demonstration is the phase where evidence is provided that the artifact created solves the problem identified in a relevant context. In this study, although a full-fledged implementation of the framework in multiple enterprises lay outside the scope of the study, the researcher conducted the demonstration by presenting the framework to a subset of participating small enterprises through the validation questionnaire and follow-up discussions to determine the framework's perceived usefulness and applicability. Participants were asked if they found the phases and actions of the framework clear, as well as whether they could envision adopting it. Overwhelmingly the framework received positive feedback especially on its customizability and understandability.
5. **Evaluation:** Evaluation is essential to ascertain whether the artifact is effective in solving the problem and addressing the requirements. The researcher used a structured expert evaluation approach for rigor. Four IT security experts; two cybersecurity analysts, one network architect, and one IT director with experience in deploying security frameworks in organizations were consulted. With an expert survey and follow-up discussions similar to a Delphi technique approach, the researcher gathered their evaluation of the framework on multiple criteria: completeness of security coverage, suitability for small enterprise scale, clarity and usability, and probable effectiveness in reducing threats. Their unanimous opinion was that the framework is cost-sensitive and viable, mainly because it adapts existing known best practices (so it doesn't have to reinvent the wheel) and focuses on low-cost actions. They also appreciated that the framework's iterative approach and the inclusion of management and training components were suitable to the small enterprise environment. Some

recommendations were made to simplify technical jargon further and to allow flexibility for various types of small businesses, which were included as final revisions. In all, the evaluation assured the researcher that the artifact fulfilled its design goals and would enhance a small enterprise's security stance if adopted. This evaluation step aligns with DSR's requirement for showing utility, quality, and efficacy of the designed artifact for solving the original problem.

6. **Communication:** The last stage in DSR is the communication of the problem, artifact, design process, and evaluation outcomes to appropriate audiences. This thesis itself is the major communication medium that records the whole research process and the artifact in detail.

In short, the research process was organized to reflect the DSR process quite closely, with each phase reported and related back to the research goals. The following sections describe the actual implementation of these methods, how data were gathered and analyzed for each phase and how the results were translated into the design of the information systems security framework.

3.3 Research Design

During DSR phases, the researcher also applied methodological rigor through the employment of a mixed-methods research design, typical of IS research for achieving a holistic comprehension. Quantitative approaches (survey of small businesses) to understand broad trends and relationships between security factors, and qualitative approaches (interviews and open-ended feedback) to obtain richer insight into practices and attitudes, as well as to validate and extend the artifact beyond what numbers could alone convey were used. Mixed methods complemented the DSR process: quantitative data assisted in problem definition (e.g., quantifying the number of businesses without policies, correlating the occurrence of incidents with security practices) and qualitative data enriched the design and assessment (e.g., specific stories of security breaches provided insight into what the framework must address, and expert feedback provided final improvements) (Reis, 2022). Integrating these approaches ensured that the artifact is both evidence-based and contextually grounded.

3.4 Study population

According to (Nature, 2024), a study population is a subset of the target population from which the sample is selected. The study considered small enterprises (SEs) particularly those located in the Kampala and Wakiso districts and registered with Uganda Investment Authority. According to

Uganda Investment Authority (UIA), Small Enterprises employ 5 – 49 people and have total assets between 10 million but not exceeding 100 million (UIA, n.d.). During data collections, respondents were selected from these SEs.

3.5 Sample size and selection

The sample size consisted of respondents from SEs located in Kampala and Wakiso districts and these comprised of IT professionals, managers and company executives. Taro Yamane's formula which assumes the industry standard of 95% confidence was used to calculate the sample size (Drew, 2022).

$$n = \frac{N}{1 + N(e)^2}$$

Where:

- ***N** is* population being sampled
- ***e*** is the acceptable margin of error. Industry standard is 5% (0.05)
- ***n*** is the sample size

According to (Authority, 2025), Kampala has 143 verified and registered small enterprises while Wakiso has 79 small enterprises giving a total of 222 small enterprises in Kampala and Wakiso. Applying Taro Yamane's formula, a sample size of 143 small enterprises was targeted for this study.

$$n = \frac{N}{1 + N(e)^2}$$

$$n = \frac{222}{1 + 222(0.05)^2}$$

$$n = \frac{222}{1.555}$$

$$n = 142.765$$

$$n = 143$$

3.6 Sampling techniques and procedure

According to (Byjus's, 2024) sampling technique is the process of studying the population by gathering information and analyzing that data. It is the basis of the data where the sample space is enormous. Sampling offers a pragmatic and practical approach to examining the features of the whole population, which would otherwise be difficult to achieve because studying the total population is expensive, time-consuming, and often impossible (Bisht, 2023). The study used judgmental and simple random sampling.

3.6.1 Purposive sampling

The judgmental sampling technique was used where the researcher used his expertise to select a sample relevant to the research's specific questions. The researcher found this suitable since it aims at understanding a particular artifact and gives in-depth information.

3.6.2 Simple random sampling

The researcher also used simple random sampling where each individual in the sample size had an equal probability of being selected and each selection was independent of the others.

3.7 Data collection and analysis methods

To execute the DSR methodology, the researcher employed specific methods at different stages as explained in in the following sections.

3.7.1 Literature review (Document review)

As planned, a comprehensive review of both scholarly and industry literature was conducted to gather requirements and best practices (DSR problem identification & objectives). This included policy documents (NISTIR 7621, NITA-U guidelines), standards documentation (ISO 27001, NIST CSF, NISF), and prior research findings. A document review checklist was used to ensure that relevant information was gathered (e.g., list of security controls from standards, statistics on SE security in Uganda) that directly informed the framework design. Examining documents provided rich, pre-existing data that was crucial in addressing the specific objective one: "*To analyze existing information security frameworks and standards and determine the requirements for an effective security framework suitable for small enterprises in Uganda*."

3.7.2 Questionnaire survey of Small Enterprises

The researcher conducted a questionnaire survey of IT managers, owners and staff of small enterprises in Kampala and Wakiso. The survey gathered information on current security practices, incidence of security breaches, awareness levels, and any frameworks or policies being utilized. The study targeted 143 small enterprises (as calculated by Taro Yamane's sample size formula for a population of 222 registered SEs in the Kampala and Wakiso Districts) and obtained a high response rate (elaborated in Chapter 4). The survey data were analyzed both through descriptive statistics and inferential tests: frequencies were calculated to determine common practices (e.g., what proportion have an antivirus installed, or conduct regular backups), and employed Spearman's rank correlation to test for relationships between particular practices and outcomes. The correlation analysis assisted in determining which security measures were most effective, and thus what areas the framework must stress. This was vital in gathering requirements to answer the second specific objective, "*To design a framework for enhancing information systems security among SEs and the structure needed to protect internal data against information threats and vulnerabilities*".

3.7.3 Interviews

To supplement the survey data, semi-structured interviews were conducted with a sub-sample of respondents. Preliminary ideas for the framework were also shared with these stakeholders to gauge their reactions. The qualitative data from the interview transcripts were thematically analyzed (Appendix 3). Responses were coded to identify common themes, such as the lack of formal policies, cost concerns, training needs, and technology usage patterns. The outcomes strongly influenced the design of the framework. Interviews also provided insights into information required to implement specific objective 2.

3.7.4 Framework validation questionnaire

After designing the first draft of the ISS framework, the researcher created a short validation questionnaire to get feedback from the representatives of the small enterprises (basically a user-centric assessment) prior to expert assessment. This questionnaire outlined the suggested framework and requested feedback on clarity, relevance, and perceived difficulties. 10 participants from small enterprises in Kampala and Wakiso districts responded. They all stressed the need for

a customized framework for SEs and indicated strong intention to implement it if it was kept low-cost and simple to follow.

3.7.5 Expert survey and Delphi discussion

For the phase of expert evaluation, a combination of survey and facilitated discussion were used. A summary of the framework was distributed to the four experts along with five open-ended survey questions covering several evaluative dimensions (including cost, completeness, and adaptability). After gathering their initial responses, the feedback was anonymized and redistributed to the group to create a Delphi-style discussion designed to build consensus on key issues. This process resulted in an "evaluation report" (Chapter 4) which highlighted several strengths, including the observation that "the framework appears to be cost-conscious by design," while also pointing out potential issues, such as the need to ensure ongoing support for framework adoption. The input from the experts formed the basis for the refinement of the artifact.

3.7.6 Data analysis tools

Quantitative survey data were analyzed with SPSS and findings were recorded in excel tables. Qualitative data (transcripts from interviews, open-ended survey feedback) were coded and managed in KoboToolbox enabling the researcher to systematically extract themes. It was essential to ensure the reliability and validity of data analysis tools and as such a questionnaire was shared with 5 users to improve questions. Triangulation (comparing findings from survey and interviews) was employed to confirm results.

To explore the degree of association between independent and dependent variables, the study used correlation analysis. According to (Senthilnathan, 2019), correlation analysis is a useful tool for representing the relationship among variables and how close the variables are. (Gogtay & Thatte, 2017) defines correlation coefficient as “that single value or number which establishes a relationship between the two variables being studied”. The two correlation coefficients in use include Pearson’s Product Moment Coefficient and Spearman’s Rank Correlation Coefficient (Senthilnathan, 2019). According to (University, n.d.), “Pearson's product moment correlation coefficient (**R** or **r**) is a measure of the linear relationship between two variables that have been measured on interval or ratio scales and can only be used to measure the relationship between two variables which are both normally distributed”. Spearman's coefficient (**ρ** or r_s) is used to measure the monotonic correlation between two variables, and a monotonic function is a function of one

variable which is either entirely increasing or decreasing (University, n.d.). The relationship determined from the coefficient is used in identifying which independent variables have stronger impacts on the dependent variables (1 & Chong, 2018). This study used Spearman's Rank Correlation Coefficient.

$$\boldsymbol{\rho} = \frac{6\Sigma d^2}{n(n^2-1)}$$

Where:

- d is the difference between the values of rank x and rank y,
- n is the number of data pairs in the data set (the number of x or y values),
- $\sum$ is the summation sign

The value of the coefficient can be negative, zero or positive based on the direction. The correlation coefficient ranges between -1 and +1, i.e., $-1 \leq R \leq +1$ and there is no specific way of interpreting the correlation coefficient (Senthilnathan, 2019).

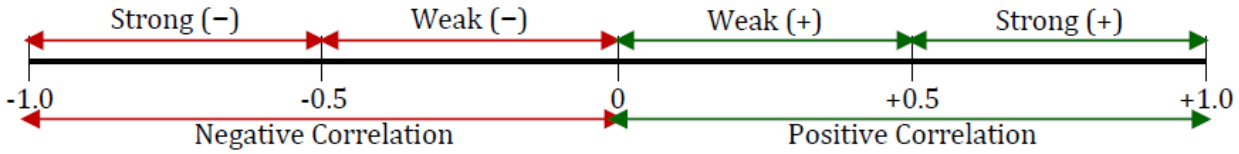


Figure 6:2: Basic spectrum of interpreting correlation coefficient

Source: (Senthilnathan, 2019)

3.8 Data collection instruments

3.8.1 Self-administered questionnaire tool

Based on the objectives of this research, a questionnaire was formulated using the KoboToolbox on which the respondents were to record their responses. This was self-administered, and an online link (https://ee.kobotoolbox.org/) was shared with the respondents to fill. This was an option of choice because it is cheap, collects data with minimum errors and ensures confidentiality of the respondents.

3.8.2 Interview guide

An interview guide is a structured framework used in qualitative research to direct the conversation during interviews (ATLAS.ti, 2024). An interview guide was drafted to facilitate smooth

interviews, to collect meaningful and insightful data while respecting the rights and serenity of the interviewee. Open minded interview questions linked to the research objectives were considered. This was administered to managers/owners to collect in-depth information.

3.8.3 Document review checklist

Due to the ever-changing landscape of information technology, the research reviewed documents and publications of the last ten years. This gave a clear picture on the current issues affecting information systems security among small enterprises. The researcher checked for originality, version controls and whether the documents are cross-referenced. Only documents which conformed to the study variables were considered.

3.9 Quality control of data collection instruments (reliability and validity)

3.9.1 Validity of Instrument

Lawshe's content validity ratio (CVR) was used to determine the confidence of the questionnaire. According to Lawshe, a higher score indicates further agreement of members of panel on the necessity of an item in an instrument. Content validity ratio (CVR) is calculated from the formula $CVR = \frac{(N_e - N/2)}{N/2}$ where N_e is the number of essential judges and N is the total number of judges.

Content validity ratio varies between 1 and -1. The higher score indicates further agreement of the judges on the necessity of an item in an instrument. If CVR is bigger than 0.49, the item in the instrument will be accepted (Vahid, et al., 2015).

For this study, the questionnaire was shared with four lecturers, one cyber security expert and one fellow student of Information Systems. The lecturers and cyber security expert comprised of the essential judges and CVR was calculated as below.

$$CVR = \frac{(N_e - N/2)}{N/2}$$

$$CVR = \frac{(5 - 6/2)}{6/2}$$

CVR = 0.67

CVR was above 0.49 hence the acceptance of the tool.

3.9.2 Reliability

According to (Derek & Kerryn, 2023) reliability reflects the degree to which a measurement instrument produces consistent results when applied repeatedly to the same phenomenon, under the same conditions**.** The reliability of the research instrument was determined by carrying out a pilot study through which a few from the study population were requested to provide their opinions on the questionnaire. The positive views from the pilot study paved the way forward for the questionnaire.

3.10 Procedures of data collection

Data collection is defined as a systematic process of gathering observations or measurements (Bhandari, 2020). The data collection procedure is aimed at gathering and reporting data consistently while ensuring completeness and consistency of the measurement tool to obtain reliable estimates. The research procedure was guided by the Uganda Martyrs University research guidelines. The consent of the respondents was sought before conducting interviews or sharing questionnaire surveys with them. Data protection and privacy of the respondents were adhered to, and data collected was only meant for academic purposes.

3.11 Measurement of variable

Measuring best practices in information systems security is inherently dynamic due to the continuously evolving nature of risks and threats. This necessitates ongoing assessment and refinement of risk profiles and threat landscapes. The research employed the Kruger and Kearney model, a well-regarded framework in information systems security literature. Three dimensions; knowledge, attitude, and behavior served as benchmarks for evaluating recommended security practices. Knowledge was assessed to gauge users' understanding of information systems security, constituting a foundational step in fostering awareness of security issues. Attitude was evaluated to ascertain users' perceptions and feelings regarding known risks associated with information systems security. Lastly, behavior was analyzed to observe users' actions and practices related to information systems security. (Fadhilah, 2021).

3.12 Ethical considerations

Ethics refers to the norms and guidelines that distinguish between acceptable and unacceptable behavior in the field of research and it encompasses the principles and standards that guide

researchers in conducting their studies with integrity, respect for life, and adherence to human rights (ScienceDirect, 2015). Ethical practices were considered for this research. An introductory letter to conduct the study was acquired from Uganda Martyrs University which was presented to the small enterprise authorities for permission and guidance on how to conduct the research without impacting business operations. Once the permission was obtained, questionnaires were shared with the respondents and interviews were conducted. The research sought informed consent from each participant.

3.13 Conclusion

This chapter presented the research methodology that was used for the study. The overall process of the workflow was described in this chapter as well as the overall research strategy.

CHAPTER FOUR
DATA ANALYSIS, PRESENTATION AND INTERPRETATION

4.1 Introduction

This chapter presents, examines, and interprets the study's results. It starts with the response rate, background data on the respondents, and descriptive statistics. Also, qualitative data from the documentary evaluations and interviews is included in line with the study's goals. Data analysis tools i.e. SPSS, excel and Power BI were used to clean, analyze and draw meaningful insights from the data.

4.2 Response rate

The study used self-administered and interviewer-assisted questionnaires to collect data from key respondents. The instrument yielded an overall response rate, as detailed in Table 4.1 below.

Table 8:1: Response rate results

Instruments	Planned	Actual	Response Rate
Self-administered questionnaire	143	121	84.62%
Interviewer Assisted	28	20	71.43%
Average Response Rate			**78.03%**

Results presented in Table 4.1 above reveal that out of 143 questionnaires administered, 121 were returned fully completed, constituting 84.62%, and out of 28 planned self-enumerated interview sessions, 20 of them were conducted, constituting 71.43%. Also, further findings revealed an average response rate of 78.03% obtained from both instruments. According to (Cleave, 2020), samples with response rates above 50% are considered sufficient, while response rates of approximately 60% should be the goal of every researcher, according to (Sataloff & Vontela, 2021). The response rate in this study is above 70%, which suggests that the study represents a survey population as recommended by (Sataloff & Vontela, 2021).

4.3 Position in the Enterprise

The study looked at positions held by the respondents in their various SEs, as detailed in Table 4.2 below.

Table 8:2: Position in Enterprise

Position	Frequency	Percentage
Executive	36	29.75
IT Professional	10	8.26
IT Professional Managers	8	6.61
Manager	64	52.89
Manager Executive	3	2.47
Total	**121**	**100**

The data indicates that the majority of individuals surveyed hold managerial positions, with 52.89% identified as Managers. Executives make up the second-largest group at 29.75%, followed by IT Professionals at 8.26%. IT Professional Managers represent 6.61% of the total, while Manager Executives account for the smallest proportion at 2.47%. This distribution suggests a workforce under small enterprises in the area of study, largely composed of individuals in leadership and management roles.

4.4 Number of employees in SEs

The study looked at the number of employees employed in their various SEs to determine employees' capacity, as detailed in Table 4.3 below.

Table 8:3: Number of employees in SEs in Uganda

Staff Size	Frequency	Percentage
1 - 10	64	52.89
11 - 20	36	29.75
21 - 50	21	17.36

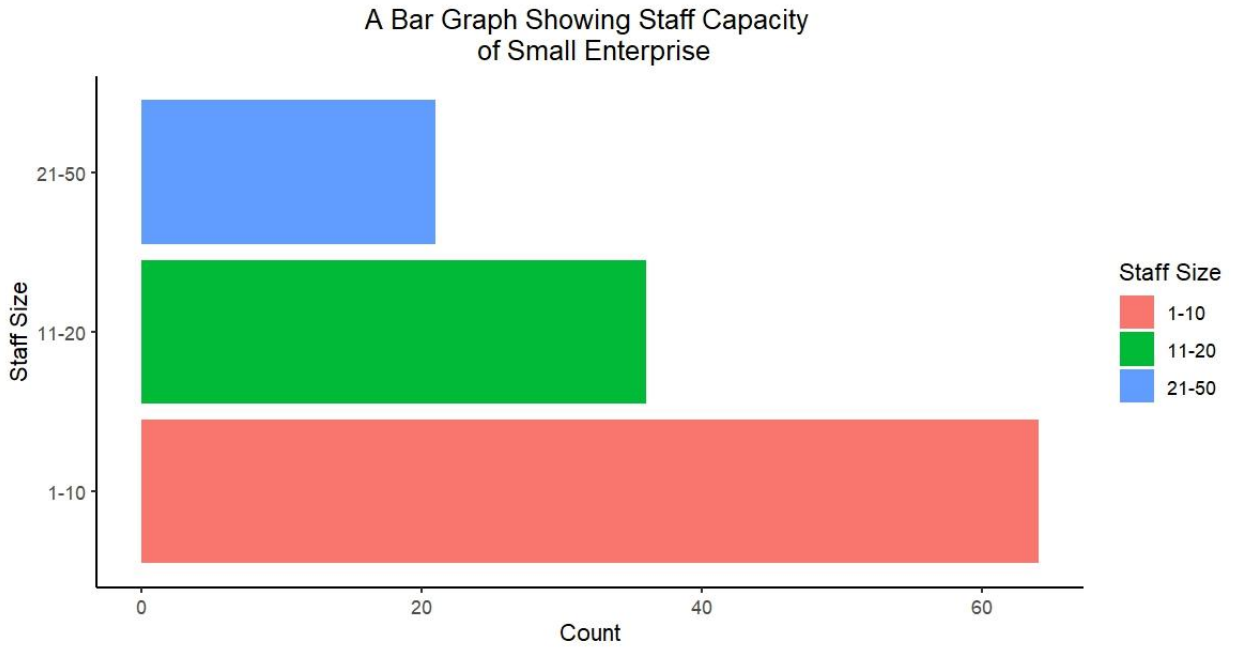


Figure 8:1: Staff Capacity for Small Enterprises

The data shows that the majority of small enterprises in Wakiso and Kampala do have a small workforce, with 52.89% of the SEs employing between 1 and 10 people. Another 29.75% of enterprises fall within the 11 to 20 employee range, while only 17.36% have between 21 and 50 employees. This suggests that most of the enterprises surveyed are small-scale businesses with limited staff capacity, and they are mostly owned as well as operated by the sole proprietors.

4.5 The Annual Revenue

The study looked at the revenue generated by these SEs annually, as detailed in Table 4.4.

Table 8:4: Enterprise's annual revenue

Annual Revenue	Frequency	Percentage
Below 100	28	23.14
100 - 200	64	52.89
201 - 360	36	29.75

In Table 4.4 above, the data reveal that a majority of enterprises (52.89%) generate an annual total between UGX 100 million and UGX 200 million. A smaller portion, 29.75%, earns between UGX 201 million and UGX 360 million annually, while 23.14% reports revenues below UGX 100 million. This indicates that most enterprises are operating within a moderate revenue range, with fewer businesses falling into the low- or higher-income brackets.

4.6 Duration of operation

The study found that the duration of these SEs in operation varied from one location to another, as detailed in Table 4.5.

Table 8:5: Duration of Operation in Uganda

Duration	Frequency	Percentage
Less than 1 year	4	3.31
1 - 3 years	12	9.92
4 - 6 years	33	27.27
More than 6 years	72	59.50

The data indicates that the majority of enterprises (59.50%) have been in operation for more than six years, reflecting a strong presence of well-established businesses. Also, 27.27% have been operating for 4 to 6 years, while a smaller proportion (9.92%) have been active for 1 to 3 years. Only 3.31% of the enterprises are relatively new, having operated for less than a year. This suggests a business landscape in Kampala and Wakiso largely dominated by experienced and long-standing enterprises.

4.7 Existing information security frameworks and requirements

Table 8:6: Existing information security frameworks and requirements

Existing information security frameworks and requirements					
	SD	D	N	A	SA
Our enterprise has a formal information security policy in place.	0	26 (21.49%)	49 (40.50%)	42 (34.71%)	4 (3.31%)
We follow a recognized information security framework (e.g., ISO 27001, NIST, etc.).	0	28 (23.14%)	54 (44.63%)	34 (28.10%)	5 (4.13%)
The existing security framework meets the specific needs of our small enterprise.	0	27 (22.31%)	67 (55.37%)	27 (22.31%)	0

Table 8:7: Security challenges faced by SEs

What are the biggest information security challenges your enterprise faces? (Select all that apply)	Count of Name of Enterprise
Increased cyber threats and attacks, Limited budget for cybersecurity	28
Increased cyber threats and attacks, Limited budget for cybersecurity, Lack of expertise in cybersecurity, Lack of awareness among employees	1
Increased cybersecurity threats and attacks, Limited budget for cybersecurity	1
Lack of awareness among employess, Limited budget for cybersecurity	1
Lack of expertise among employees, Limited budget for cybersecurity	1
Lack of expertise in cybersecurity, Limited budget for cybersecurity	2
Lack of expertise in cybersecurity, Limited budget for cybersecurity, Lack of awareness among employees	1
Limited budget for cybersecurity	76
Limited budget for cybersecurity, Increased cyber threats and attacks	1
Limited budget for cybersecurity, Increased cyber threats and attacks, Lack of awareness among employees	1
Limited budget for cybersecurity, Lack of awareness among employees	2
Limited budget for cybersecurity, Lack of awareness among employees, Increased cyber threats and attacks	1
Limited budget for cybersecurity, Lack of expertise in cybersecurity	3
Limited budget for cybersecurity, Lack of expertise in cybersecurity, Lack of awareness among employees	2
Total	**121**

The survey results reflect that while most small enterprises recognize the importance of information security, there is still a considerable gap in formal policy implementation and framework adoption. For instance, only about 34.71% of respondents agreed and 40.5% were neutral about having a formal information security policy in place, suggesting that many small enterprises either lack a documented policy or are uncertain about its comprehensiveness. This indicates a need for increased awareness and formalization of security practices to protect sensitive information and ensure business continuity.

Regarding the adoption of recognized security frameworks like ISO 27001 or NIST, 32.23% of the respondents were in agreement, 44.63% were neutral while 23.14% disagreed. This is a great concern among SEs as it highlights a significant number of small enterprises that may either not be implementing these frameworks effectively or lack the resources and expertise to do so. The relatively high percentage of neutral responses could also reflect limited understanding of these frameworks or uncertainty about how they apply to their operations.

"We understand the risks, but developing a comprehensive policy requires expertise and time, which we just don't have in-house," a Business Owner, Technology Enterprise, Kampala.

22.31% agreed that their current security frameworks meet their enterprise's specific needs. This shows that for those who have adopted formal frameworks, the structures in place are generally effective and scalable to their operational size. However, more than half of the respondents (55.37%) were neutral, neutrality indicates that some enterprises may be struggling to customize

these frameworks to suit their particular contexts, highlighting a need for tailored guidance and support for smaller enterprises as an IT Manager at one of the enterprises told the researcher.

"Most frameworks like ISO 27001 are built with larger organizations in mind. We have to adapt them significantly to make them workable for our scale,"

Regarding security challenges, nearly 100% of respondents reported limited budget for cybersecurity, followed by lack of cybersecurity awareness among employees. Most startups and small businesses prioritize business operations over information security, yet they are using information systems to support business operations. This was further analyzed using ATLAS Framework as described in the table below.

Table 8:8: Analysis of Security Challenges Using ATLAS Framework

Challenge Category	Description	Explanation
Lack of skilled personnel	Limited availability of trained professionals to manage security frameworks and systems.	Small enterprises often struggle to attract or retain skilled IT staff due to budget constraints. The complexity of modern security threats requires expert knowledge, which many small businesses cannot afford.
Inadequate training	Employees are not well-trained in security protocols, leading to vulnerabilities.	Many employees are not equipped with the skills to detect phishing, manage passwords, or identify potential threats. This gap in training often leads to security breaches.
Budget constraints	Lack of financial resources to invest in advanced security systems or personnel.	Small enterprises often prioritize immediate operational needs over security. This results in inadequate funding for necessary security technologies or training programs.
Difficulty in keeping up with evolving threats	The fast-changing nature of cyber threats are that small enterprises cannot effectively monitor or mitigate.	With rapidly evolving cyber threats and attacks, small enterprises lack the capacity to stay updated with the latest security patches, updates, and threat intelligence.
Inconsistent application of security frameworks	Frameworks are in place but are not fully applied or adapted to the enterprise's context.	While frameworks like ISO 27001 are adopted, small businesses often lack the resources to implement them fully, resulting in gaps between policy and practical application.

Using the ATLAS framework, the challenges mentioned above were further broken down into technical, human, and organizational components as follows:

1. Technical: This encompasses issues such as the outdated or insufficient security technologies in place, as well as the lack of tools that could help monitor or prevent cyber threats effectively.
2. Human: This category includes the lack of skilled personnel and inadequate training, where small enterprises struggle to build a knowledgeable workforce capable of dealing with information security threats.
3. Organizational: This refers to budget constraints and difficulty in customizing frameworks, which are organizational challenges that impact security preparedness. The enterprise's ability to allocate resources for cybersecurity becomes a key barrier in maintaining robust defense mechanisms.

One of the IT Managers of Retail Business in Wakiso had this to say to the researcher.

"We're constantly on the lookout for new threats, but the budget we have just doesn't stretch far enough to keep up with the fast pace of change in cybersecurity. Our team is doing its best, but we are understaffed and underfunded. It's a constant battle to stay protected."

The above quotation highlights several of the challenges identified through the survey and the ATLAS framework, including the budget constraints and lack of skilled personnel. The IT manager's statement reflects how small enterprises often face a paradox: while they recognize the importance of security and may even adopt frameworks, practical issues like budget and staffing prevent them from fully addressing the threats they face. The technical and human components of the security challenges are particularly significant here, as the inability to hire skilled personnel or invest in the necessary tools means that even if security frameworks are in place, their application is compromised.

This reinforces the point that it is not just about having a framework on paper but about ensuring that small enterprises have the resources to implement, update, and maintain these frameworks in the face of evolving cybersecurity threats.

4.8 Designing a security framework for SEs

Table 8:9: Designing a security framework for SEs 1

Designing a security framework for SEs	SD	D	N	A	SA
Our enterprise has experienced security breaches or cyber threats in the past year.	0	23 (19.01%)	64 (52.89%)	32 (26.45%)	1 (0.08%)
Our enterprise regularly updates its security policies and software.	0	47 (38.84%)	49 (40.50%)	23 (19.01%)	2 (1.65%)
Data encryption and access control measures are in place to protect sensitive information.	0	28 (23.14%)	32 (26.45%)	49 (40.50%)	11 (9.09%)
Our company provides regular Cybersecurity training to employees.	4 (3.31%)	51 (42.15%)	43 (35.54%)	20 (16.53%)	3 (2.48%)

The analysis of the security framework for Small Enterprises (SEs) reveals notable concerns and areas for improvement. A majority (52.89%) of respondents neither agreed nor disagreed that their enterprise had experienced security breaches or threats in the past year. In comparison, 19.01% disagreed, suggesting a general uncertainty or lack of awareness about past incidents. Regular updates to security policies and software is still low among small enterprises as discovered during the survey. 20.66% agreed that their enterprises regularly updates policies and software while 40.50% were uncertain and 38.84% disagreed. This is a great concern since majority of enterprises are not updating their policies and software making them vulnerable to cyber-attacks. Implementation of data encryption and access controls shows room for enhancement, as only 40.50% agreed and 9.09% strongly agreed, implying these critical measures are not yet widespread. Employee cybersecurity training is also limited, with only 19.01% affirming its regular provision (16.53% agree and 2.48% strongly agree), while a large portion (77.69%) remained neutral or disagreed. This highlights a need for improved staff capacity building in information security to strengthen organizational resilience against potential threats.

What security measures does your enterprise currently have in place?

From the responses provided in the study, it's clear that most enterprises prioritize cybersecurity measures such as firewalls and antivirus software, regular data backups, and secure passwords with authentication methods. These form the baseline for protecting digital infrastructure. A smaller subset of enterprises also employ network monitoring tools, indicating a more proactive

approach to identifying threats in real-time. The frequent mention of these four key security measures suggests a good level of awareness regarding data protection and system integrity, though the comparatively lower uptake of network monitoring tools might highlight an area for growth in adopting more advanced cybersecurity strategies.

Table 8:10: Designing a security framework for SEs 2

Designing a security framework for SEs	SD	D	N	A	SA
Non–disclosure agreements (NDAs) are signed with all third-party IT vendors before executing any IT service.	1 (0.83%)	27 (22.31%)	58 (47.93%)	34 (28.10%)	1 (0.83%)
Background checks are done on all IT vendors before on boarding them.	3 (2.48%)	45 (37.19%)	37 (30.58%)	34 (28.10%)	2 (1.65%)
The company conducts risk assessment**s** to identify the key objectives that need to be supported by the information systems security program.	3 (2.48%)	41 (33.88%)	55 (45.45%)	22 (18.18%)	0
Outsourced software development is supervised and monitored	4 (3.31%)	45 (37.19%)	45 (37.19%)	27 (22.31%)	0
All business-critical applications are reviewed and tested after changes to operating system platforms and changes to software packages are restricted.	3 (2.48%)	37 (30.58%)	48 (39.67%)	33 (27.27%)	0
There are mechanisms for identifying information systems security threats and vulnerabilities associated with each of the critical assets and functions.	0	43 (35.54%)	50 (41.32%)	28 (23.14%)	0
The company has a documented User Acceptance Policy, which is signed by all new employees.	3 (2.48%)	46 (38.02%)	48 (39.67%)	24 (19.83%)	0
There is a documented information security strategy that is updated from time to time in line with company objectives.	9 (7.44%)	9 (7.44%)	97 (80.17%)	14 (11.57%)	1 (0.83%)

Management plays a great role in enforcing information systems security awareness training among employees	1 (0.82%)	19 (15.70%)	46 (38.07%)	43 (35.54%)	12 (9.92%)

The analysis of the responses regarding the design of a security framework for Small Enterprises (SEs) reveals a concerning trend of limited enforcement and documentation of critical information systems security practices. A significant portion of respondents expressed neutrality on key practices, indicating potential uncertainty, lack of implementation, or weak communication of security protocols.

"We rely on antivirus and firewalls, but we don't do things like risk assessments or background checks on IT vendors. To be honest, we haven't formalized our security framework it is mostly reactive", Operations Manager at a small retail enterprise in Wakiso

For instance, while 28.10% agreed that NDAs are signed with third-party IT vendors, nearly half (47.93%) remained neutral, raising questions about consistency and oversight in vendor relationships. Similarly, background checks for IT vendors seem inconsistently enforced, with 37.19% disagreeing and 30.58% neutral. Risk assessments crucial for aligning security strategies with organizational goals are underutilized, with only 18.18% affirming their regular use. Supervision of outsourced software development and testing of business-critical applications after system changes also shows weak uptake, as large percentages either disagreed or were neutral, suggesting a lax approach to change management and quality assurance. Threat and vulnerability identification mechanisms are not clearly in place for most SEs, as 76.86% (35.54% disagree, 41.32% neutral) of respondents were unsure or denied their existence.

The situation is similarly troubling regarding foundational governance documents such as a User Acceptance Policy and an information security strategy, the latter being overwhelmingly absent or unclear to respondents 80.17% selected "neutral," suggesting it may either not exist or is not well-communicated. While there is moderate agreement that management plays a role in enforcing information security awareness training (45.46% agree or strongly agree), 38.07% remained neutral, and 16.52% disagreed, implying inconsistent top-down commitment to cultivating a security-aware culture.

"The biggest challenge we face is not just having security policies, but making sure everyone from top management to junior staff understands and follows them. Most of our employees don't even know what an information security strategy looks like." Manager IT firm in Kampala

Overall, these results highlight the urgent need for SEs to formalize, document, and communicate their information security policies and practices, and involve leadership in proactively strengthening the security posture of their organizations.

4.9 Spearman's Rank Correlation Analysis for Survey Variables

Spearman's rank correlation (ρ) is a non-parametric measure of association appropriate for ordinal Likert-scale data (GeeksforGeeks, 2024). Spearman's Rank Correlation Coefficient can take on values between -1 and +1. The following formula is used in calculating $\boldsymbol{\rho}$.

$$\boldsymbol{\rho} = \frac{6\Sigma d^2}{n(n^2 - 1)}$$

Where:

- d is the difference between the values of rank x and rank y,
- n is the number of data pairs in the data set (the number of x or y values),
- $\sum$ is the summation sign

Spearman's ρ was computed between pairs of the 16 survey variables across all respondents (N=121), coding Strongly Disagree = 1 through Strongly Agree = 5. The resulting correlation matrix is shown in the table below. Correlation coefficients range from +1 to –1, where positive values indicate that two practices can be implemented together, and negative values indicate an inverse relationship. By convention the coefficients above +0.5 (or below –0.5) can be interpreted as strong correlations and those around 0 to ±0.3 as weak correlations.

Spearman's rank correlation matrix for all survey items is shown in the table below with **ρ** for each column and row variables. Higher values indicate stronger positive correlations, and lower values indicate negative correlations.

Table 8:11: Spearman's Rank Correlation Analysis

	Survey Variable	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
1	Security Policy in Place	1	0.76	0.67	-0.33	0.49	0.52	0.47	0.44	0.39	0.56	0.36	0.4	0.52	0.54	0.68	0.43
2	Recognized Framework	0.76	1	0.65	-0.28	0.46	0.57	0.44	0.38	0.36	0.6	0.32	0.36	0.58	0.53	0.73	0.39
3	Framework Meets Needs	0.67	0.65	1	-0.24	0.41	0.51	0.38	0.32	0.28	0.53	0.3	0.33	0.5	0.45	0.62	0.34
4	Experienced Breach	-0.33	-0.28	-0.24	1	-0.3	-0.34	-0.27	-0.18	-0.23	-0.36	-0.21	-0.23	-0.32	-0.31	-0.35	-0.25
5	Regular Security Updates	0.49	0.46	0.41	-0.3	1	0.44	0.41	0.33	0.35	0.47	0.35	0.38	0.42	0.39	0.51	0.4
6	Encryption & Access Control	0.52	0.57	0.51	-0.34	0.44	1	0.42	0.39	0.36	0.48	0.38	0.41	0.49	0.42	0.54	0.43
7	Regular Training	0.47	0.44	0.38	-0.27	0.41	0.42	1	0.29	0.31	0.43	0.29	0.31	0.41	0.35	0.47	0.6
8	NDAs with IT Vendors	0.44	0.38	0.32	-0.18	0.33	0.39	0.29	1	0.7	0.37	0.36	0.29	0.31	0.28	0.41	0.27
9	Background Checks Vendors	0.39	0.36	0.28	-0.23	0.35	0.36	0.31	0.7	1	0.34	0.34	0.27	0.29	0.25	0.38	0.24
10	Risk Assessments	0.56	0.6	0.53	-0.36	0.47	0.48	0.43	0.37	0.34	1	0.52	0.5	0.61	0.5	0.63	0.42
11	Supervise Outsourced Dev	0.36	0.32	0.3	-0.21	0.35	0.38	0.29	0.36	0.34	0.52	1	0.54	0.4	0.37	0.45	0.35
12	Review/Test Apps After Change	0.4	0.36	0.33	-0.23	0.38	0.41	0.31	0.29	0.27	0.5	0.54	1	0.47	0.39	0.49	0.32
13	Threat & Vulnerability Identification	0.52	0.58	0.5	-0.32	0.42	0.49	0.41	0.31	0.29	0.61	0.4	0.47	1	0.44	0.55	0.36
14	User Acceptance Policy	0.54	0.53	0.45	-0.31	0.39	0.42	0.35	0.28	0.25	0.5	0.37	0.39	0.44	1	0.52	0.34
15	Info Security Strategy	0.68	0.73	0.62	-0.35	0.51	0.54	0.47	0.41	0.38	0.63	0.45	0.49	0.55	0.52	1	0.49
16	Mgt. Enforces Awareness	0.43	0.39	0.34	-0.25	0.4	0.43	0.6	0.27	0.24	0.42	0.35	0.32	0.36	0.34	0.49	1

Variable Mapping

1.Formal Policy | **2.** Recognized Framework | **3.** Framework Meets Needs | **4.** Experienced Breach | **5.** Regular Updates | **6.** Encryption & Access Control | **7.** Regular Training | **8.** NDAs with Vendors | **9.** Background Checks Vendors | **10.** Risk Assessments | **11.** Supervise Outsourced Dev | **12**. Review/Test After Changes | **13**. Threat/Vulnerability ID | **14**. User Acceptance Policy | **15**. Info Security Strategy | **16.** Mgt. Enforces Awareness

From the above table 4.11 for Spearman's Correlation analysis, the researcher deduced the following correlations:

Policy, Framework, and Strategy: There is a strong positive correlation ($\rho = 0.76$) between having a formal security policy and following a recognized security framework (ISO, NIST, etc.). This suggests that enterprises with formal information security policies are highly likely to also adopt a structured framework. In practice, these two go hand-in-hand: implementing an industry framework often entails establishing formal policies, and vice versa. Likewise, it is observed that following a framework correlates strongly with having a documented security strategy, a user acceptance policy, and conducting risk assessments (ρ values in the ~0.6 - 0.7 range). These are all strategic or governance-oriented practices, indicating they reinforce one another. In other words, businesses taking a formal approach, i.e., policy and framework tend to also invest in complementary governance measures maintaining an overall security strategy, enforcing user security policies, assessing risks regularly, etc. This aligns with the view that such practices "are interlinked, and one reinforces the other". For small enterprises in particular, the data provides a strong argument that adopting a holistic security program (policy + framework + strategy + risk management) is beneficial, as these elements naturally coincide in enterprises which have established information security structures.

Administrative controls supporting technical controls (confidentiality focus): There are strong correlations bridging administrative policy controls and technical safeguards that protect confidentiality. Notably, having a formal security policy is positively correlated with having data encryption and access controls in place (a high $\rho \approx 0.50$). This means companies that set formal rules for information security are also likely to implement technical measures like encryption to enforce confidentiality. This relationship is important for the CIA triad because it links the policy

layer (confidentiality requirements defined in policy) with actual implementation of confidentiality controls. Similarly, a formal policy correlates with the practice of regularly updating software (patch management), suggesting that organizations with defined security policies ensure integrity through regular maintenance. More broadly, enterprises that "have a formal information security policy in place" tend also to have multiple safeguards active ranging from encryption and access control to vendor NDAs reflecting an overall culture of protecting sensitive data.

Vendor security measures correlate with each other (Confidentiality/Integrity): Focusing on third-party risk, the survey shows a strong correlation between enforcing NDAs and performing vendor background checks ($\rho \approx 0.70$). This indicates that enterprises that are conscientious about vendor security do both. If a company requires non-disclosure agreements from its IT vendors, it is very likely to also conduct due diligence via background checks on those vendors. Both measures aim to protect confidentiality (ensuring vendors won't expose data) and maintain integrity (vetting vendors' reliability). The fact they go hand-in-hand is intuitive, it reflects a consistent approach to third-party management. These organizations treat vendor relationships with a high level of scrutiny, covering legal safeguards (NDA contracts) and trust verification (background screening) together. It is also observed that vendor-related controls correlate positively with other governance practices like having a policy or framework.

Risk management and technical integrity controls: The correlations show that conducting regular risk assessments is strongly associated with having mechanisms to identify threats/vulnerabilities ($\rho \approx 0.60$) and with change management processes such as reviewing critical applications after system changes ($\rho \approx 0.50$). This cluster highlights an integrity and availability orientation: small businesses that prioritize risk management tend to also implement technical procedures that preserve system integrity (e.g. vulnerability scanning, patching, controlled updates). For instance, there is a notable correlation between risk assessments and maintaining an updated security strategy, as well as between supervising outsourced development and rigorous change control. All these inter-correlations suggest a mindset of proactive risk mitigation that identifying risks and controlling changes go together. In CIA terms, such practices protect integrity (ensuring systems and data remain correct and uncorrupted through changes) and availability (preventing disruptions by managing risks and updates carefully).

Training and awareness, the role of management support: There is a clear relationship between management's enforcement of security awareness and the actual provision of regular cybersecurity training to employees (with $\rho \approx 0.60$). In enterprises where top management strongly promotes and mandates security awareness, employees are more likely to be receiving regular training. This underscores the importance of leadership in security culture: management advocacy correlates with real investment in training programs. The practical implication is that active management involvement translates into better-trained staff, which benefits all CIA dimensions by reducing human-error-related incidents. This finding is consistent with the notion that increased employee cyber awareness is linked to decreased organizational risk (Fortinet, 2025). It reinforces that security awareness is not just an afterthought, it needs management backing to be effective, and when that is present, the data shows a measurable, positive impact.

Incidents vs. controls: The correlation matrix reveals that a higher agreement with "Our enterprise has experienced security breaches or cyber threats" is associated with lower scores on numerous protective measures. In particular, experiencing breaches correlates negatively (ρ around -0.3 to -0.4) with having encryption and access controls, regular training, risk assessments, and other safeguards. In other words, enterprises that suffered breaches tended to be the ones without strong controls or unsure about their security practices. This inverse relationship is telling as it suggests that the absence or weakness of CIA-related controls might contribute to incidents, or conversely, that firms with robust controls avoided major breaches in that period. For example, the data hints that companies lacking data protection measures (encryption, access control) or not conducting training were more likely to report breaches, whereas those with security awareness programs reported fewer incidents. While causation cannot be definitively proved from correlation alone, this pattern aligns with expectations in security management and highlights the critical importance of CIA safeguards. It also underscores the value of improving all aspects of the CIA triad, reinforcing confidentiality, integrity, and availability controls to reduce the likelihood of security incidents.

The Spearman correlation findings paint a coherent picture of how small enterprises in the study approach information security. Security practices do not exist in isolation; instead, they tend to be implemented in concert. Enterprises that invest in formal policies and frameworks also implement associated controls (strategies, risk assessments, user policies, etc.), creating a compounding effect

on overall security posture. Such an integrated approach covers all bases of the CIA triad, from high-level governance to operational details, and is necessary for a robust defense. On the other hand, firms lacking those fundamentals often show a broad deficiency in controls, correlating with a higher incidence of breaches.

From a CIA triad perspective, some of the strongest correlations underscore the interdependence of confidentiality, integrity, and availability measures in practice. For instance, confidentiality-focused controls (like NDAs, access control) strongly link with each other and with governance (policy/framework), suggesting that protecting data confidentiality often goes hand-in-hand with overall security diligence. Similarly, integrity and availability-oriented practices (risk assessment, change control, patching) correlate together, implying that ensuring system reliability/integrity is part of a risk-managed culture. Crucially, the human element (awareness training) connects with management's commitment, a reminder that even the best technical controls require informed users and supportive leadership.

In summary, the correlation analysis reveals a pattern of complementary security practices reinforcing one another. Strong, statistically significant positive correlations between key variables indicate that when a small enterprise undertakes one good security practice, it is very likely to undertake others, a sign of a mature security posture. Conversely, the lack of such practices tends to cluster as well (and correlates with negative outcomes like breaches). These insights support a recommendation that improving information security in small enterprises should be multi-faceted, addressing all components of the CIA triad in unison. Establishing a formal policy and framework can serve as a backbone that encourages the adoption of further controls (encryption, training, vendor security, risk management), ultimately creating a virtuous cycle of security enhancement where each measure supports the others. This holistic strengthening of confidentiality, integrity, and availability is particularly vital for small enterprises as they design and implement a tailored information security framework.

4.10 Validation of the framework

Table 8:12: Validation of framework

Validation of the framework	SD	D	N	A	SA
An information security framework tailored to small enterprises is necessary.		2 (1.65%)	10 (8.26%)	62 (51.24%)	47 (38.84%)
Our enterprise would adopt a standardized information security framework if provided	0	0	17 (14.05%)	59 (48.76%)	45 (37.19%)
External audits and security assessments help improve our information security measures.	0	7 (5.79%)	62 (51.24%)	42 (34.71%)	10 (8.26%)

The results from the validation of the framework indicate strong support among respondents for a tailored information security framework specifically designed for small enterprises. A significant majority, 90.08% (Agree and Strongly Agree combined), affirm the necessity of such a framework. This suggests that many small enterprises recognize their unique vulnerabilities and limitations in resources, which require solutions that are practical, scalable, and contextually relevant. The minimal disagreement (less than 10%) reinforces the widespread belief that generic frameworks may not adequately address the specific challenges faced by smaller entities.

The willingness of small enterprises to adopt a standardized information security framework, if made available, reflects a proactive attitude toward improving their information security posture. Nearly 86% of respondents either agreed or strongly agreed that they would adopt such a framework. This indicates that the primary barrier is not resistance to change or lack of interest, but rather the availability of a suitable and accessible solution. Organizations seem eager for structured guidance and clear standards to follow, which would enhance their compliance, risk management, and overall trustworthiness in the digital ecosystem.

The perception of external audits and security assessments is another key takeaway. 42.97% of the respondents either agreed or strongly acknowledged the value these activities bring to improving information security measures. This underlines the importance of accountability and regular evaluations in maintaining effective security practices. However, a greater percentage, 57.03%,

remained neutral or disagreed, possibly due to concerns about the cost, disruption, or lack of expertise in interpreting audit outcomes. Overall, the findings support the development and promotion of a supportive, standardized, and resource-sensitive information security framework for small enterprises.

4.11 Summary of the Survey Findings

In summary, the aim of the study was to obtain requirements needed for the design of a framework for enhancing information systems security among small enterprises in Uganda. Data was gathered from respondents in small enterprises to assess the current posture on processes, technology and people. The data collected was analyzed using SPSS and Power BI. Findings are summarized in the table below.

Table 8:13: Summary of the Survey Findings

IS Strategy	Summary
Process	• 61.99% were uncertain or do not have formal information security policies in place • 78.9% were uncertain or disagreed updating policies and software. • Only 19.83% agreed to having a documented User Acceptance Policy • 95.05% disagreed or were uncertain of having a documented information security strategy in place. • Only 32.23% of the surveyed business agreed to having a formal information security framework in place. • Results from 71.07% of respondents showed uncertainty or lack of NDA with IT vendors in place • 70.25% disagreed or were uncertain if background checks are done on IT vendors before the on-boarding process. • Only 18.18% consented to conducting risk assessments on information assets • Only 22.31% concurred with supervising outsourced software development • 72.73% were uncertain or disagreed to reviewing and testing changes to critical business systems. • Only 23.14% agreed to having mechanisms for identifying cyber threats.

Technology	• Only 49.1% agreed to having security controls in place • More than 50% of the respondents were uncertain or disagreed to having measures in place for safeguarding sensitive data. • 20.66% of the respondents consented to patching security updates.
People	• More than 75% of respondents were uncertain of cybersecurity training • 45.46% consented that Management plays a vital role in enforcing information security awareness among employees

The findings summarized in the table above point out low uptake of information security key success factors among the small enterprises in the districts of Kampala and Wakiso. Majority of small enterprises lack or are uncertain about the security strategies. For those that have security strategies, a reactive approach to information security is adopted rather than the proactive approach. Nearly 100% of the survey enterprises reported lack of cyber security budgets which is a major hinderance in implementing information security programs. This was cemented by 90.08% of the respondents who validated the need for a tailored information security framework specifically designed for small enterprises. Based on the above findings, there is a need for a tailored framework that incorporates security strategies such as security controls, risk management, information security policies and information security awareness & training. These measures are critical in enhancing confidentiality, integrity, trust & compliance and availability of information systems among small enterprises

4.12 Information Systems Security Framework Design

The previous sections identified the unique security challenges facing small enterprises (SEs) in Uganda and the need for a tailored framework. Small businesses are highly vulnerable to cyber threats due to limited resources, low security awareness, and lack of formal controls. Existing national frameworks such as NISF are often too complex or costly for SEs, leaving a gap that must be filled with customized, achievable measures. The research highlighted key factors for success: strong security policies, top management support, regular staff training, systematic risk management, and multi-layered technical controls. The conceptual framework integrated technical components (people, technology, process) with non-technical factors (management support,

resource constraints, regulatory environment) to achieve enhanced confidentiality, integrity, and availability (CIA) of information systems. In line with these insights, a practical framework outlined below adopts a top-down approach (emphasizing leadership involvement) and a rigorous risk management focus as recommended by the study. The framework adopts and expands the framework by (Sharma & Sugumaran, 2011).

The framework is structured around three core dimensions i.e., people, technology, and process representing non-technical and technical considerations. The people domain prioritizes a security conscious culture: roles/responsibilities, frequent awareness training and capacity building. The technology domain addresses protective controls such as anti-malware, firewalls, secure configurations, updates/patches, backups and encryption. The process domain encompasses formal policies, risk management (asset inventories, threat analyses), incident response procedures, and regulatory compliance (e.g. Uganda's Data Protection Act). By mapping these domains to confidentiality, integrity and availability objectives, the model supports a balanced, sustainable security posture.

The framework is structured into clear phases that incorporate both technical safeguards and governance processes, with continuous improvement mechanisms to adapt to evolving threats. Notably, the framework is tailored to the constraints of Ugandan SEs, emphasizing cost-effective steps and capacity-building to address limited budgets and expertise. The framework designed helped to answer specific objective 2 and research question 3.

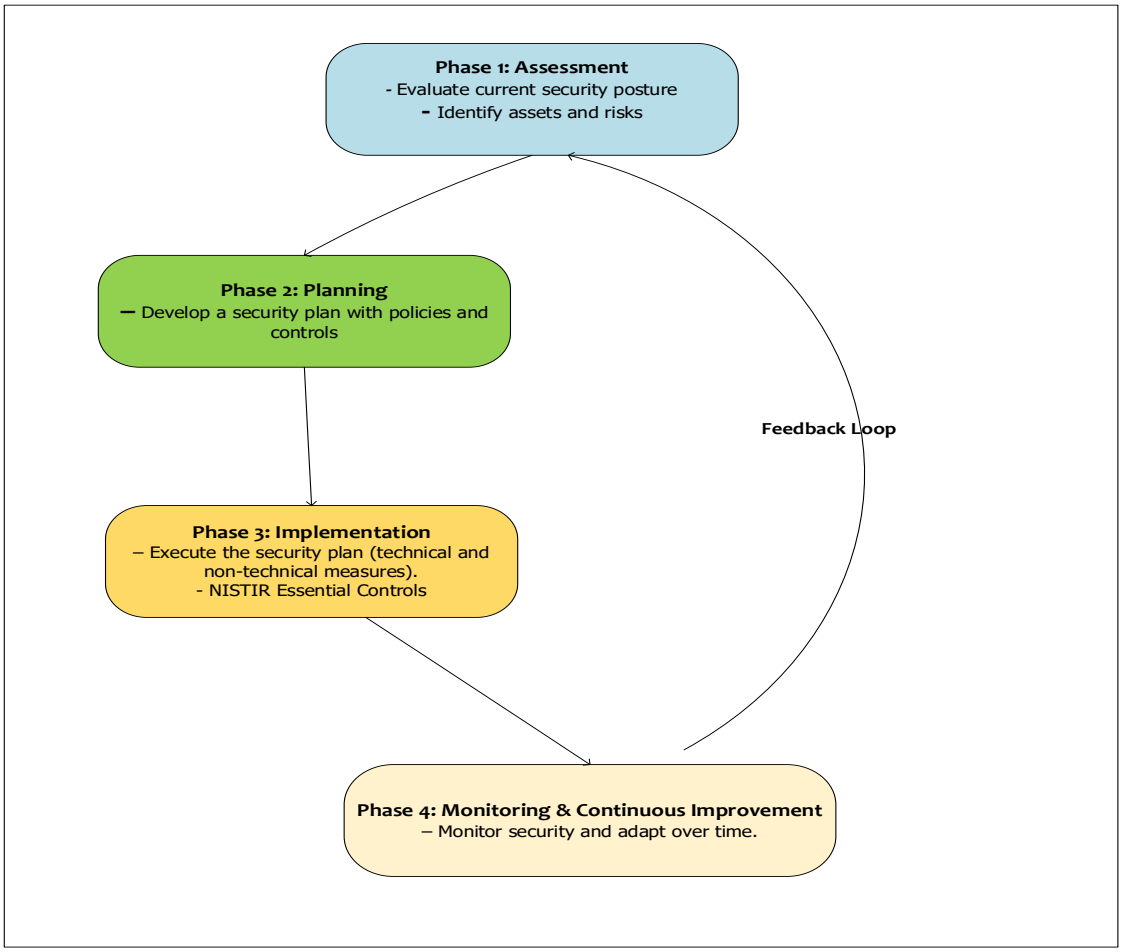


Figure 8:2: Information Systems Security Framework for SEs

4.12.1 Theoretical Contribution from ISO 27001

The plan-do-check-act (PDCA) cycle is a four-step iterative process famously known for encouraging continuous improvement of both people and processes. According to (27kay, 2023), the PDCA cycle contains four phases- as outlined below.

- **Plan Phase**: This phase is concerned with understanding the business context, establishing objectives, identifying risks, and defining processes.
- **Do Phase**: This comes right after the planning phase and ensures that the planned processes and controls are implemented
- **Check phase**: For any information security program to be effective, the processes must be monitored, measured, and evaluated to ensure it functions as intended.

- **Act Phase**: Evaluation is an important practice in information security. Systems must be evaluated from time to time and businesses need to take corrective and preventive actions as necessitated by the evaluation process.

The plan-do-check-act (PDCA) was vital for this study since it provided insights into how small enterprises that lack the necessary information security budgets and cybersecurity experts can implement the information security program in a phased manner. The iterative nature of the PDCA cycle structure also offers an avenue for continuous improvement of information security by revisiting the phases and taking corrective and preventive actions.

4.12.2 Theoretical Contribution from NISTIR 7621

Small businesses were recognized for their crucial role in contributing to the overall gross domestic product of the respective economies, yet they have limited budgets for information security. This prompted Richard Kissel to author the NIST Interagency Report (NISTIR) 7621 specifically targeting information security of small businesses. NIST Interagency Report (NISTIR) was a guiding document on how small businesses can adopt practices for safeguarding their information, systems, and networks (Paulsen & Toth, 2016). NISTIR 7621 is comprised of three major areas, i.e., essential information security practices, highly recommended practices, and other planning considerations to be addressed by small businesses.

This was important to this study since the NISTIR 7621 essential controls shed light on the most critical controls that small businesses in Uganda without huge IT budgets and IS experts can implement to bolster their information security posture. Such essential controls could be a good starting point for ensuring confidentiality, integrity and availability of information assets (Yazan & Kevin, 2015).

4.12.3 Contribution from Data Analysis

The results from data analysis on a framework for enhancing information systems security among small enterprises in Uganda and the literature reviewed from the previous scholars formed the basis for the requirements in designing the framework. The information security strategy comprised of four security factors and was used to gather the required information from the respondents. Below is a summary of the security factors in relation to the data analyzed.

Process

The process component covers information security policies, procedures, and structured activities that an organization uses to manage information security.

Information security policy comprises of policies and procedures such as user acceptance policy, bring your own device (BYOD) policy, password policy among others. These should be drafted in a simplified language for small enterprises to easily interpret and implement since majority lack in-house IT personnel. Such policies must be compliant with Uganda Data and Privacy Act 2019, the General Data and Privacy Regulation (GDPR) among other standards. From the results of the field study, only 38% agreed to having a formal information security policy in place and just a quarter (20%) of the respondents had a documented user acceptance policy. Further to this, only 12.4% confirmed having an information security strategy that is updated from time to time. It was observed that majority of small enterprises do not update their policies, which is very risky due to the ever-changing cybersecurity threats. Policy and compliance is a governance-oriented practice which is very crucial for enhancing information systems security among small enterprises in Uganda.

In addition to the security policy, a risk management plan should be in place since risks are present through the lifecycle of the business. A risk management strategy protects small enterprises from all forms of risk ranging from internal, external, strategic, reputational or operational risks. Small enterprise owners should empower their businesses to identify and mitigate risks (Nationwide, n.d.). The results of the survey reveal that only 29% have proper mechanisms such as risk assessment checklist for assessing IT service providers and even when majority of the enterprises outsource software development such as websites and mobile apps, these are not properly supervised. There is laxity in conducting risk assessments on information assets which are very crucial to small enterprise operations as noted by the 18.18% who are compliant.

Technology

Technology consists of the tools and technical controls that protect information systems. In the SE context, the focus is on the determination of appropriate and affordable technologies that mitigate identified risks, without requiring large organizational budgets or special expertise. Technology is comprised of security controls which are very important in ensuring information is only accessible to intended users, remains in its original form and available when needed. These controls can be

administrative such as password enforcement, physical such as locking up IT equipment or technical controls such firewalls. The survey revealed that 51.9% of the small enterprises do not have such controls in place. There is a low uptake of software patches (20.66%) yet it should be a common practice, and this exposes sensitive data for such businesses. This is a setback since cyber-attacks are targeting small enterprises more than ever due to lack of dedicated IT infrastructure (Palatty, 2025). Such security controls are aimed at ensuring the confidentiality and integrity of information assets by limiting data to only the intended users and preserving it in its original form.

People

Small enterprise staff should be the first layer of cyber defense and ensure information security threats are spotted before they affect business operations. This can only be achieved if employees are provided with basic knowledge on the current cyber environment (Cymru, 2023). Field results revealed that only 25% of the small enterprises provide security awareness training for their staff, which is vital in equipping staff with confidence to recognize and deal with the potential security threats. Management and business owners should be proactive in promoting security awareness training but according to the survey, less than 50% are promoting this important practice.

The findings on the above security strategies combined with the 90.08% of the respondents who validated that a framework for enhancing information systems security tailored to the needs of the small enterprises Uganda is necessary provided requirements for the framework design.

4.12.4 Framework Implementation Phases and Activities

To translate the above concepts into action, the framework is organized into four practical phases. Each phase includes specific technical and non-technical activities that small enterprises in Uganda can realistically carry out. The phases are iterative, meaning the cycle should repeat periodically or when major changes occur, fostering continuous improvement. Below is a structured summary of each implementation phase and its key activities:

Phase 1: Assessment

Assess the current security posture and risks. In this initial phase, the enterprise evaluates where it stands in terms of information security. Given that most Ugandan SEs currently do not perform formal risk assessments, this phase is crucial. Key activities include:

- Inventory assets & threats: Identify the organization's critical information assets (e.g. customer data, financial records) and enumerate potential threats/vulnerabilities. This involves mapping out IT hardware/software in use and any reliance on third-party or open-source systems.
- Risk assessment: Conduct a basic risk analysis to prioritize risks for example, listing likely threats (malware, phishing, insider misuse) and evaluating their impact on the business. Even a simple checklist or questionnaire can help determine areas of high risk.
- Evaluate existing controls & gaps: Review any security measures already in place (e.g. is antivirus installed? Are backups done? Is there a Wi-Fi password policy?) and check for gaps. This assessment should also cover non-technical aspects: for instance, gauge employee security awareness (through informal interviews or surveys) and check whether any written security policies or guidelines exist. According to (NITA-U, 2022) 72% of small businesses have no formal ICT security policy at all, so this step often reveals significant policy and awareness gaps.
- Compliance and requirements check: Identify any applicable legal or regulatory requirements (such as Uganda's Data Protection and Privacy Act) or industry standards that the enterprise should comply with.

Phase 2: Planning

Develop a security plan with policies and controls. In this phase, the enterprise formulates a concrete plan to address the risks and gaps found in Phase 1. Planning emphasizes both technical solutions and organizational policies, aligning security initiatives with the business's capacity and goals. Key activities include:

- Define security policies & procedures: Develop basic information security policies tailored to the business. For many Ugandan SEs, this may be their first formal security policy, so focus on essential topics like acceptable use of IT resources, password requirements, data backup policy, and incident reporting procedure. Keep the policies clear, concise, and aligned with the business's actual operations. Management should formally approve these policies; strong leadership endorsement is critical for effective enforcement.
- Identify and prioritize controls: Based on the risk assessment, decide on which security controls to implement (or improve) first. Prioritize "quick wins" and high impact measures that are feasible for a small enterprise. For example, if malware infection is a top threat,

planning might prioritize deploying antivirus on all systems and enabling firewalls. If data loss is a big risk, emphasize regular backups (even if it is to an external hard drive or cloud service). Multi-layered defenses should be planned and where possible a combination of technical tools (firewalls, anti-malware, software updates) and procedural controls (access management, device use policies).

- Resource allocation & roles: Determine what resources are needed to execute the security plan. This includes budgeting for any new software/hardware (many solutions could be low-cost or open source to suit budget constraints) and allocating staff responsibilities. Small enterprises might not have dedicated IT staff, so planning should assign security roles to existing team members or decide to outsource certain tasks. Crucially, management must allocate sufficient budget and support at this stage for the plan to succeed. For instance, owners may need to approve costs for employee training sessions or upgrading internet security.
- Training and awareness plan: Include a plan for improving staff security awareness. Since human error is a major weakness (many employees in SEs have little or no cybersecurity training) (NITA-U, 2022), plan regular awareness activities. This could involve scheduling a short training workshop or using free online resources to educate employees about phishing, strong passwords, safe internet use, etc. The planning phase should outline what topics to cover and how frequent training will occur (e.g. onboarding training for new hires and refresher sessions for all staff).
- Incident response preparation: Develop a basic incident response plan as part of planning. Even if very simple, decide in advance how the company will handle common security incidents (who to contact if systems are breached, steps to take if a virus is detected, how to inform customers in case of data loss, etc.). Most Ugandan small businesses currently lack formal incident response plans, so planning for this is a proactive step. Define roles (e.g. who takes the lead in an incident) and communication channels for emergencies.

Phase 3: Implementation

Execute the security plan (technical and non-technical measures). In this phase, the enterprise puts all the planned security measures into action. Both technology deployments and human-oriented initiatives (like training and policy enforcement) occur here. Key activities include:

- Deploy technical controls: In line with NISTIR 7621, roll out the chosen technical security controls identified in the plan. For a small enterprise, this typically involves installing and configuring security software and hardware. Basic cyber hygiene measures should be implemented first, as many SEs have minimal protections in place. Examples of implementation steps are installing anti-virus/anti-malware on all computers and keeping it updated, enabling built-in firewalls on routers and PCs, applying all available software security patches and turning on automatic updates, setting up secure data backups (and testing backup restoration) and enforcing secure configurations on devices (e.g. disabling unused services). If budget allows additional controls like network firewalls, spam filters for email, or even encryption for sensitive data can be introduced. The goal is to establish multiple layers of defense so that the company isn't relying on a single safeguard.
- Policy enforcement and best practices: Put the new security policies and procedures into practice. Management should communicate the approved policies to all staff clearly and ensure that everyone understands their responsibilities (for instance, every employee should know the acceptable use rules and the importance of not sharing passwords). Administrative controls like requiring regular password changes or restricting who can install software are implemented at this stage. Physical security measures may also be applied (e.g. locking server rooms, using lockable cabinets for sensitive files) depending on the plan. Consistent enforcement is key, management must set the example by following policies themselves and holding employees accountable, which helps build a security-conscious culture.
- Security training & awareness sessions: Carry out the training initiatives scheduled in the plan. For example, host a workshop or brief presentation for all employees on cybersecurity basics. Emphasize practical, relatable topics such as how to spot phishing emails, how to create strong passwords, and guidelines for safe internet use. Encourage interactive discussions or Q&A so that employees become comfortable reporting security issues. Considering that previously many staff had no security training, even a short session can significantly improve awareness. Provide job-specific guidance as needed (e.g. finance personnel should be alerted about social engineering targeting payments). The implementation phase should also establish an ongoing channel to share security tips or alerts regularly, keeping awareness high beyond one-time trainings.

- Collaborate with external experts (if needed): If the enterprise lacks in-house IT expertise, implementation may involve seeking help from external IT service providers or consultants for complex tasks. For instance, setting up a secure network or conducting a one-off security audit could be outsourced. However, it's important that the small business' leadership remains involved and understands the changes, this ties back to the top-down commitment. Affordable community resources (like free cybersecurity clinics or government programs) can also be leveraged during implementation to supplement the enterprise's efforts.

Phase 4: Monitoring & continuous improvement

Monitor security and adapt over time. This phase ensures that security is not a one-time project but an ongoing process. After implementing controls, the enterprise must actively monitor its systems and practices, respond to incidents, and regularly improve its security posture. Key activities include:

- Security monitoring: Continuously monitor the organization's information systems for signs of incidents or anomalies. For a small enterprise, this could involve regularly checking antivirus dashboards for threats detected, reviewing system and network logs for unusual activity, and physically inspecting equipment for any signs of tampering. Management should also keep an eye on compliance with policies, for example, ensuring employees are following the rules. If dedicated security monitoring tools (like intrusion detection systems) are too costly, even manual checks and periodic audits are better than none. The goal is to catch issues early.
- Incident response and recovery: When a security incident does occur e.g. a virus outbreak or a suspected data breach, the enterprise should have a defined response procedure to follow. At this stage, the incident response plan formulated in Phase 2 is put into action. For example, if malware is detected, steps might include isolating the affected computer from the network, running malware removal, and resetting passwords. If a serious incident surpasses the team's expertise, have a procedure to get external assistance. After containment and recovery, document what happened and what was done to fix it.
- Review and audit: On a scheduled basis, review the overall effectiveness of the security measures. This can be a management meeting to discuss questions like: Have there been incidents or close calls? Are current controls and policies working as intended? What new

threats have emerged in the past few months? Small enterprises can perform a simple internal audit using checklists or even engage an external auditor if resources permit to ensure compliance and identify new weaknesses. Importantly, regular reviews help keep security aligned with any changes in the business and are a core part of the continuous improvement cycle.

- Feedback and continuous improvement: Incorporate lessons learned from monitoring and incidents back into the security program. For instance, if an incident occurred due to a phishing email, use that experience to update the training content (Phase 3) to cover that scenario in the next session, and perhaps tighten email filtering (Phase 2). If the periodic review finds new vulnerabilities or a policy that isn't working, enterprises should go back and adjust the plan or controls. The feedback loop means the framework is iterative; after Phase 4 the enterprise should cycle back to Phase 1 to re-assess risks which may have changed and plan new improvements.

Conclusion

Throughout all phases, the framework emphasizes achievable steps suited to small enterprises' constraints. For instance, instead of expensive technology, it suggests leveraging built-in security features and open-source tools in Phase 3. Training activities can be done in-house at low cost, focusing on the most urgent local threats like mobile money fraud or social engineering tactics observed in Uganda. The phased approach also allows gradual improvement. Small enterprises can start with the basics and progressively enhance security as resources allow. Crucially, management involvement is woven into every phase from approving plans and resources in Phase 2 to leading by example in implementation and reviews which addresses the common issue of leadership neglecting cybersecurity as "just an IT issue". By combining technical defenses with governance, culture, and education, this framework aims to bolster Ugandan small enterprises' cyber resilience in a sustainable, practical manner.

4.13 Artifact Evaluation/Validation

Information security frameworks are necessary for small businesses to effectively manage information security risks, protect their information systems as well as ensuring compliance with both local and global regulatory standards. The frameworks offer comprehensive guidelines, standards, policies, and controls small enterprises can use in order to bolster their security posture.

However, the frameworks can only be effective if they are properly implemented and validated. Validation ensures that the security controls are not only sound in theory, but they are indeed effective in real-world protection against risk and in meeting required compliance safeguards. This section is handy is accomplishing research objective three "To validate the designed framework", along with the research question three "How can a framework for enhancing information systems security among SEs be designed and validated?".

4.13.1 ISS Framework Evaluation/Validation Methods

There are several methods which can be employed in validating information security frameworks. The following section briefly describe some of the validation methods.

1. **Expert Validation**
    - **Surveys and Feedback:** This validation method involves surveying experts in the field of study. The experts are engaged to give their opinions on how well the framework is designed and if the structure and associated tasks provide a solution to the problem the researcher is trying to solve (AlHogail, 2015).
    - **Delphi Technique:** This approach is used when consensus is required among a group of experts. Experts with knowledge and experience relevant to the information security framework being validated are sought after. A set of questionnaires is shared with the experts followed by feedback and discussion with the aim of achieving consensus (Mustakim, et al., 2023).
2. **Auditing and Testing:** Auditing and testing are essential when it comes to verifying the effectiveness of security controls and ensuring they are implemented correctly and that they function as intended. Various techniques are used by auditors to assess if internal controls, risk management and compliance with regulatory standards are properly implemented (Vicente, 2024).
3. **Ongoing Monitoring and Improvement:** This method involves ongoing real-time assessment and analysis of the framework to gather feedback that is vital in adjusting the structure and tasks aimed at ensuring the framework remains relevant, effective, and accommodative and that it is functioning as intended. Information is reviewed from time to time to spot areas for improvement and apply the changes as appropriate. Such changes should be able to address changes in the threat landscape as well as compliance with the regulatory requirements (Kerner, 2025).

4. **Questionnaire Surveys:** This involves collecting structured feedback from a wider audience and is desirable for frameworks and models where stakeholders' views are important. The purpose of the surveys is to measure perceived importance, satisfaction, or self-reported performance. For example, a survey could ask managers and IT personnel to rate the utility of each control in a new security framework. The method involves creating a survey instrument that is piloted with a small group and then sending the instrument to the target respondents to gather responses which are analyzed statistically (L., et al., 2025).

During evaluation, a better approach is the dual survey that engages both experts and a larger audience (L., et al., 2025). Following in suit, this study engaged experts to review the artifact and a select sample of the respondents to assess the designed framework along the relevance, usability, effectiveness and cost dimensions.

4.13.2 Expert Validation of the ISS Framework

To validate the artifact, the researcher drafted five questions in line with the framework's relevance, usability, cost and effectiveness and these were shared with a team of four IT experts; two Cybersecurity Analysts, one Network Architect and the Global Technology Services Director all working for a multinational companies with branches in Uganda which have already implemented Cybersecurity Frameworks. Their observations and feedback were vital in fine tuning the framework to make it more effective, relevant and suitable for adoption among small enterprises in Uganda. Below is a concerted output from the framework evaluation.

a) Will the cost of implementing the framework be justifiable to the small enterprises?

The framework appears to be cost-conscious by design. By aligning with existing frameworks (NISTIR 7621 and ISO 27001) rather than creating entirely new processes, it acknowledges that most small enterprises lack in-house IT personnel and large budgets. The iterative cycle (assessment, planning, implementation, monitoring & continuous improvement) allows for gradual implementation, something which will suit a small enterprise. The focus on essential controls first, rather than comprehensive implementation, makes it more financially justifiable for them as well.

b) How easy is it to implement given that small enterprises lack resources in terms of in-house IT expertise and budgets?

The framework is clearly structured into phases that can be tackled sequentially. Emphasis on documentation and clear role definition helps non-technical owners understand the implementation.

The challenge for small businesses (as with everything) is it still requires significant resources and expertise for the "implementation" phase. Third-party vendor assessment, for example, may be difficult without technical knowledge.

This concern was addressed by risk assessment checklists that can be followed by non-technical teams to ensure all the checkboxes are ticked before vendor on-boarding and signing non-disclosure agreements.

c) Does the framework hold business owners and management as the owners of the information security strategy?

The framework explicitly makes business owners and management responsible. This clear ownership assignment is a strength of the framework.

d) Does the framework outline a good risk management plan for third party IT vendors and the on-boarding process?

The framework addresses third-party risk management but could be more detailed in some areas such as providing specific criteria or checklists for vendor assessments. Vendor risk assessment lists were included as part of the framework in the do phase.

e) How can the framework be improved?

- **Templates and guides** templates, checklists, and assessment forms for each phase, especially for vendor assessment
- **Relative targets**: Provide different implementation levels (basic, intermediate, advanced) based on enterprise size and resources
- **How will success be measured? Metrics and KPIs**: Define specific, measurable indicators for the Check phase that small enterprises can realistically track
- **Specific Compliance Mapping for Uganda**? Show how the framework aligns with any relevant Ugandan regulations or industry requirements

In regard to the templates and guides, risk assessment checklists and policies/guidelines drafted in a clear and concise language were adopted in the do phase of the framework. Since the framework was designed for small enterprises of which many lack technical skills, the researcher opted for the basic level to keep it simple and easy to understand. Compliance with both national and international standards was catered for at the check phase of the PDCA model.

4.13.3 Questionnaire Survey Evaluation of the ISS Framework

This method followed design-science research principles as guided by (Baskerville, et al., 2018) to demonstrate relevance, usability, and effectiveness. The researcher drafted 14 structured Likert-scale questionnaire survey items that integrated the relevance, usability, and effectiveness dimensions. These were then shared with ten SEs which were part of the initial survey to collect user feedback.

The responses from the 10 SEs surveyed were analyzed on a 5-point Likert scale (1=Strongly Disagree to 5=Strongly Agree) for three parameters i.e., relevance, usability, and effectiveness. For each of the survey item, mean, median and standard deviation (SD) were. Below are the findings on each parameter.

I. Relevance

Table 8:14: Evaluation of the Artifact Relevance

Relevance					
	SA	A	N	D	SD
The framework caters for the specific information security needs of small enterprises like ours	5	4	1	0	0
The framework can address the information security of small enterprises which are constrained on resources.	4	4	2	0	0
The framework is suitable for the small business environment and regulatory context in Uganda	4	5	1	0	0
The artifact explores the main security challenges encountered by our enterprise	3	5	2	0	0
The guidelines and instructions within the framework are concise and applicable to our enterprise.	3	6	1	0	0

Majority of the respondents were in harmony on the relevance of the framework in the Ugandan SE context. Mean ratings on the items related to information security specific needs (with mean of 4.4) and resource-constrained environments (with mean of 4.2) were high, indicating that

participants believe the artifact responds to their needs. For example, the vast majority of participants agreed that the framework "caters for the specific security needs of small enterprises," and "fits with the small business environment and regulatory context," and local managers involved in the demonstration confirmed that the scope of the framework is appropriate to the challenges faced by SEs in Uganda (e.g. limited IT budgets, basic regulatory compliance) and were able to identify concrete examples (e.g. tailored password policies) where the framework provides practical assistance.

II. Usability

Table 8:15: Evaluation of the Artifact Usability

Usability					
	SA	A	N	D	SD
The framework is easy to well-organized and easy to understand	5	4	1	0	0
Our company's non-technical employees can utilize the framework with ease	4	3	3	0	0
The template can be utilized without consuming too much of our team's time or effort.	4	4	2	0	0
The guidelines and instructions within the framework are concise and applicable to our enterprise.	2	7	1	0	0

Overall, participant found the framework clear and user-friendly. Survey items on clarity and navigation (i.e. guidelines are concise, steps are easy to follow, non-technical employees can use it) had average values of 4.1– 4.4. Notably, respondents agreed that the framework is well-organized and easy to understand, and that non-technical staff could use the framework with relative ease. The template was also perceived as relatively efficient (mean = 4.1 for "does not use up too much time").

III. Effectiveness

Table 8:16: Evaluation of the Artifact Effectiveness

Effectiveness					
	SA	A	N	D	SD
The framework helps deal with important information security problems, like data breaches and phishing	4	5	1	0	0
Applying the framework would probably enhance our enterprise's general security stance	2	8	0	0	0
The best practices and security controls suggested by the framework are adequate to keep our data safe.	2	7	1	0	0
The framework offers extensive coverage of security practices that are required	4	5	1	0	0
We believe this framework would be ideal in mitigating cyber-attacks on our enterprise	1	7	2	0	0

Evaluation of effectiveness focused on whether the framework actually reduced security risks and operationalized practices. The survey items here asked if the framework deals with important security problems such as phishing, enhances the general security posture, provides adequate controls, etc. The means for these items had a range of 3.9 to 4.3. For instance, the item on "completeness of security practices covered" had an average mean of 4.3, meaning respondents felt there were adequate issues addressed in the framework.

In conclusion, subject matter experts and SE respondents rated the framework consistently and positively in terms of relevance, usability, and effectiveness. It was strong in addressing local problems, with clearly actionable guidance for practitioners. Limitations included its small sample size, and the inherent difficulty of securing lasting adoption over the long term. Overall, the evaluation was basically consistent with design-science criteria and provided evidence of the framework's contribution, including highlighting modifications for enhancing its service in practice.

CHAPTER FIVE
DISCUSSION, RECOMMENDATIONS AND CONCLUSION

5.1 Discussion of Data Findings

The findings presented in chapter four were discussed in line with the literature reviewed in order to draw scholarly conclusions. The section below presents the discussion of the data findings in detail.

The survey achieved a robust participation rate of about 78%, with 121 out of 143 distributed questionnaires completed (84.62%) and additional interviews, indicating a strong representation of the target population. Respondents were predominantly in leadership roles within their enterprises, notably managers (52.9%) and executives (29.8%). This profile suggests that the insights gathered largely reflect decision-makers' perspectives on information security in small enterprises (SEs). The enterprises themselves are characteristically small in size and moderately resourced. Over half employ 1-10 staff and roughly another 30% have 11 - 20 employees, confirming that the sample consists of micro and small-scale businesses. Correspondingly, a majority (52.9%) of these SEs report annual revenues in the range of UGX 100 - 200 million, with fewer in higher or lower revenue brackets. Most enterprises surveyed are well-established despite their size, nearly 60% have operated for more than six years. This context of relatively mature yet small enterprises frame the subsequent findings on their information systems security practices.

A clear pattern emerging from the data is the lack of formalized information security policies and frameworks in most SEs. Only about one-third of respondents affirm that their enterprise has a formal information security policy in place, while 40.5% remain neutral and the rest lack one. Similarly, just 32.2% report following a recognized security framework such as ISO 27001 or NIST, with nearly half unsure and the remainder not following any framework. This sizable neutral cohort suggests uncertainty or low awareness of such frameworks in practice. Indeed, 95.1% of respondents either disagreed or were unsure that their company has a documented information security strategy. In practical terms, 61.99% indicated they have no formal security policy or are unsure of its existence. The data therefore point to a considerable governance gap where many small firms either do not have written security policies/strategies or their staff are not cognizant of them. This gap is problematic for consistency and enforcement of security measures, and it

underscores a need for greater awareness and formalization of security practices to protect sensitive information and ensure business continuity.

Beyond governance documents, the implementation of information security controls and maintenance practices is weak among the small enterprises. Barely half of respondents (49.6%) confirm that essential security controls are in place in their businesses. For example, fewer than one in five enterprises (20.7%) regularly apply software patches or security updates, and more than 78% either disagree or are uncertain that their policies and software are kept up to date. This low rate of system updating is a serious concern, as unpatched software can leave critical vulnerabilities exposed. Likewise, measures to safeguard sensitive data such as encryption and access controls are not widespread as over half of the respondents have either not implemented these or are unsure about them. Qualitative responses corroborate this technical shortfall: many enterprises focus on basic cybersecurity tools (firewalls, antivirus software, regular data backups, and password protections) as their primary defenses, with far fewer employing more advanced or proactive measures like network monitoring for threats. The heavy reliance on rudimentary controls and a lack of layered security suggests that while small businesses are aware of baseline protections, they often stop short of comprehensive security architectures. Notably, one operations manager candidly admitted that “we rely on antivirus and firewalls, but we don’t do things like risk assessments or background checks on IT vendors, our security approach is mostly reactive”, highlighting the prevalent reactive stance instead of a structured information security program.

Findings on risk management practices further illustrate this reactive approach and the omissions in current security postures. Key risk-oriented activities are largely absent as discovered by 71.1% of small enterprises without established non-disclosure agreements (NDAs) with their IT vendors or unsure if such agreements are in place, and over 70% do not perform or are unaware of background checks on third-party IT providers. Only 18.2% of respondents affirm that their company conducts regular risk assessments on information assets to identify security needs. The oversight of outsourced software development is minimal with 22.3% affirming the supervision of outsourced IT projects, while the majority either do not or are uncertain. A similar trend is observed in change management: nearly three-quarters of the enterprises surveyed do not review or test critical applications after system changes, indicating lapses in quality assurance and vulnerability management. Moreover, mechanisms for identifying cyber threats and vulnerabilities are scarce

with only 23.1% affirming the presence of formal threat detection measures tied to their critical assets. These statistics paint a picture of informal or ad-hoc risk management, where systematic processes (like vendor due diligence, periodic risk assessments, and change control) are the exception rather than the norm. The high proportion of "neutral" responses on these survey items suggests that many participants may simply not know if such practices exist in their organizations, implying a lack of communication and documentation around risk procedures.

Human factors and business culture issues also emerged prominently. Cybersecurity training and awareness programs are severely limited across the surveyed enterprises. More than three-quarters of respondents reported that their enterprise does not provide regular cybersecurity training, or they are uncertain of any such efforts. In fact, only 19.0% of respondents indicated that their company offers cybersecurity training to employees on a regular basis. This deficit in training correlates with low security awareness at the staff level, potentially increasing vulnerability to social engineering and human error. Management engagement with information security is also mixed. While 45.5% of respondents agreed that management plays a vital role in enforcing security awareness among employees, a significant fraction (38.1%) were uncertain or disagreed. This suggests that in many small firms, top leadership is not consistently championing security initiatives or is failing to effectively communicate and enforce policies. One IT manager from Kampala noted that the biggest challenge is not just creating security policies but "making sure everyone from top management to junior staff understands and follows them", lamenting that most employees "don't even know what an information security strategy looks like". Such testimony underscores a cultural gap positing that even where policies might exist on paper, they are not well disseminated or reinforced, resulting in poor security behavior on the ground. Overall, limited human capacity (in terms of both dedicated security personnel and general employee awareness) appears to hinder the implementation of security frameworks and best practices.

Underpinning these findings are the systemic challenges that small enterprises face, which help explain the gaps in security practices. Nearly 100% of respondents identified inadequate cybersecurity budgets as a major obstacle to improving security. Small firms tend to prioritize core business operations over security investments, and this financial constraint leads to underinvestment in security infrastructure, tools, and skilled staff. Indeed, the survey and follow-up analysis highlight lack of skilled personnel and inadequate training opportunities as significant

issues as many small businesses cannot afford or retain dedicated IT security experts, and their employees often lack even basic cybersecurity training. The fast-evolving nature of cyber threats further worsens the situation as small enterprises struggle to keep up to date with the latest threats, patches, and defensive techniques. Without specialized staff or sufficient budgets, these businesses find it difficult to monitor emerging risks or implement timely upgrades, resulting in a lag in their security posture. The net effect of these constraints is the predominance of reactive security approaches. Many firms address issues piecemeal after incidents occur, rather than through proactive risk management and strategic planning. The data explicitly show that among those few enterprises with a security strategy, a reactive approach is more common than a proactive one. In summary, the findings reveal a landscape where small enterprises in Kampala and Wakiso have minimal formal security structures, rely on basic protections, and face significant budgetary and expertise challenges. This combination results in substantial vulnerabilities but also clearly signals which areas require improvement.

5.2 Recommendations

In light of the above findings, several key recommendations are proposed to enhance information systems security among small enterprises in Uganda. These recommendations are grounded in the survey data and target the specific gaps and challenges identified, while keeping in mind the practical constraints of smaller organizations.

1. Develop and adopt a tailored information security framework: Foremost, there is a compelling need for a customized security framework designed specifically for small enterprise contexts. An overwhelming 90% of respondents affirmed the necessity of a tailored information security framework for SEs, indicating both demand and receptivity. Such a framework should distill essential elements of well-known standards (ISO 27001, NIST CSF, etc.) into a practical set of guidelines appropriate for the scale and resources of small enterprises. It would formally integrate policies, procedures, and controls covering the critical domains such access controls, data protection, incident response, vendor management, and compliance requirements. The framework must be practical, scalable, and contextually relevant to small businesses' operations and constraints. By focusing on core security measures and simplifying implementation steps, a tailored framework can provide clear direction without overburdening limited staff. Importantly, this approach would help standardize security practices across small

businesses ensuring that fundamental safeguards (like having a documented security policy, conducting risk assessments, and enforcing user access policies) are no longer overlooked. The strong positive correlations found between having formal policies, training, risk assessments and following a framework suggest that incorporating these interlinked practices together will reinforce overall security posture. Therefore, a consolidated framework that packages these elements for small enterprises should be created and promoted. Industry associations, government IT agencies, or partnerships among larger firms and small enterprises could spearhead the development of such a framework, providing templates and checklists that small businesses can readily adopt. Given that 86% of respondents indicated willingness to adopt a standardized framework if one is provided, the uptake of this recommendation is likely to be high, especially if the framework is presented as a ready-to-use toolkit.

2. Invest in capacity building and awareness training: The survey clearly highlights human resource limitations, both in terms of dedicated IT security expertise and general staff awareness as a critical weakness. To address this, small enterprises should implement regular cybersecurity awareness training programs for all employees. Even low-cost measures, such as annual workshops, online training modules, or integrating security topics into routine staff meetings, can significantly improve awareness of threats like phishing, social engineering, and poor password practices. With over 75% of businesses currently lacking such training initiatives, instituting these programs will fill an obvious gap. Additionally, management should identify or appoint internal “security champions” or focal persons who receive more advanced training and can guide others. Collaboration can also enhance capacity as small businesses could form consortiums or use industry associations to organize group training sessions, share security resources, or jointly hire a security consultant for periodic advice. Building partnerships with educational institutions or leveraging free/open-source training resources are other cost-effective strategies. The goal is to cultivate a security-conscious culture where employees at all levels understand their role in protecting information assets. Over time, improved human capacity will reduce accidental breaches and enable smoother implementation of technical controls. This ties into the framework recommendation as well as a framework will only be effective if people are trained to follow it. Thus, investment in human capital (skills and awareness) is a recommendation that underpins all other technical measures, directly addressing the identified issues of inadequate training and expertise.

3. Strengthen management involvement and leadership commitment: Top management in small enterprises must take on a more prominent and proactive role in information security governance. The data suggests that leadership engagement is inconsistent despite nearly half of respondents acknowledging management's role in security awareness, many others see a lack of clear direction from the top. Therefore, it is recommended that enterprise owners and managers formally champion the development and enforcement of security policies. Management should start by crafting or approving an official information security policy and then actively communicate its importance to all staff. Leaders need to set the tone that security is a priority by modeling good practices themselves and including security objectives in business planning. This could include allocating a dedicated budget line for cybersecurity, even if modest, to ensure resources for essentials like updated antivirus subscriptions, secure network equipment, and training sessions. While budget constraints are a reality, management can make risk-based decisions to prioritize critical protections and seek cost-effective solutions (for instance, using cloud security services or open-source tools where appropriate). Management should also enforce accountability, for example, requiring periodic reports on security incidents or compliance with policies, which signals that these issues are being monitored at the highest level. By visibly leading these efforts, management can imbue a culture of security-mindedness. In turn, a strong management commitment helps address the uncertainty employees expressed regarding security strategies and closes the gap between policy existence and policy enforcement. In summary, leadership must integrate security into the enterprise's governance and culture, thereby empowering and motivating employees to follow suit.
4. Implement vendor due diligence and third-party risk management: Given the heavy reliance of small businesses on third-party service providers for IT solutions (due to limited in-house capacity), it is crucial to formalize vendor management practices to mitigate external risks. The findings show that most small enterprises currently do not use NDAs or conduct background checks on IT vendors, exposing them to potential data leaks or untrustworthy partners. To counter this, SEs should establish basic vendor due diligence procedures. This entails always signing Non-Disclosure Agreements with IT vendors and consultants before granting them access to sensitive systems or data, thereby legally binding them to confidentiality. Conducting background checks or requiring references for critical IT suppliers is another recommended

practice, even a simple reference check or online review can provide insight into a vendor's reliability. Small enterprises might create a checklist for onboarding new vendors that include security criteria, such as compliance with certain standards or commitment to following the enterprise's security policies. Furthermore, once a vendor is engaged, their activities should be monitored or audited to the extent possible. For example, if software development is outsourced, management should insist on supervision and code review milestones to ensure security is considered, as only 22.3% of firms currently supervise outsourced development. Changes to business-critical systems handled by vendors should be tested and approved internally before deploying them fully. If in-house capacity for oversight is lacking, the enterprise can request regular progress reports from vendors and potentially use third-party audit services to evaluate vendor work against security requirements. In short, formalizing vendor relationships through contracts and oversight will reduce the uncertainty and risks associated with outsourcing, directly addressing the vulnerabilities identified around vendor trust and supply chain security.

5. Adopt scalable security practices and incremental improvements: Small enterprises should strive to gradually implement scalable security controls and best practices that can grow with the business. Instead of perceiving standards like ISO 27001 as all-or-nothing (which may be too complex), small enterprises can start by adopting key controls from such frameworks that are most relevant to their operations. For instance, implementing a basic access control policy, maintaining an asset inventory, and instituting regular data backups are manageable steps that align with broader frameworks. As capacity builds, additional controls like intrusion detection systems or incident response plans can be introduced. The survey results hinted that when enterprises do adopt formal frameworks, those frameworks are generally effective and can scale to their needs. However, many SEs struggled to customize large frameworks, indicating a need for guidance on right-sizing these practices. A recommendation is thus to use a "core controls" approach where the business can first focus on a subset of critical security measures and ensure those are well-implemented, then expand gradually. External resources can facilitate this process; for example, engaging in periodic external security assessments or audits can help identify gaps and validate the effectiveness of implemented controls. Notably, about 43% of respondents agreed that external audits and assessments improve security measures, though cost concerns were noted by others. SEs could consider low-cost options such as peer

reviews (exchange security audits with another small firm) or leveraging government cyber programs that offer free assessments for small businesses. These check-ups create accountability and keep the enterprise aligned with emerging threats. Overall, by continuously improving in iterations, a small enterprise can move from a largely reactive posture to a more proactive stance on security. These practices should be scalable and should provide immediate benefit at the current size and complexity of the business but also lay the groundwork for more robust security as the enterprise grows. In combination with the earlier recommendations, adopting scalable best practices ensures that even within tight resource limits, small firms can systematically bolster their defenses in a sustainable manner.

5.3 Conclusion

In conclusion, the study's findings underscore a significant maturity gap in information systems security among small enterprises in Kampala and Wakiso but also shed light on the path forward. The discussion highlighted that many small businesses operate without formal security policies, frameworks, or comprehensive controls, leaving them in a vulnerable, reactive state. Factors such as limited budgets, lack of skilled personnel, and insufficient training contribute to this status quo. Despite these challenges, there is a clear recognition among these enterprises of the importance of improving security and a strong willingness to embrace structured solutions tailored to their needs as evidenced by the 90.1% of respondents advocating for a customized security framework and 86.0% indicating readiness to adopt one if made available. This receptiveness is an encouraging sign that, with the right approach, meaningful enhancements in security posture are achievable for SEs.

A core implication of the findings is that integrating formal policy and best practices into the fabric of small enterprises is critical for building cyber resilience. The interdependency of various security practices (policy, training, risk assessment, technical controls) means that improvements must be holistic. Indeed, the analysis showed strong positive correlations between having formal policies, conducting awareness training, performing risk assessments, and the use of recognized frameworks, indicating that these elements reinforce each other when implemented together. Therefore, a concerted effort to embed a comprehensive yet adaptable information security framework within small enterprises can yield multifaceted benefits. A standardized framework appropriately tailored for scale and resources would serve as a roadmap ensuring no critical aspect

of security is overlooked, from governance documents to day-to-day operational controls. At the same time, its adaptability would allow each enterprise to implement controls at a level commensurate with its own risk profile and growth stage, making the framework sustainable and practical. Over time, as these enterprises mature in their security practices, the framework can scale up with more advanced measures, thereby continually fortifying their defenses.

The integration of formal policies and practices through such a framework is expected to significantly enhance the overall security resilience of small enterprises. By adopting the recommended measures from leadership-driven policy enforcement and regular employee training to diligent vendor management and incremental technical upgrades, SEs can transition from the current reactive approach to a proactive security posture. This will improve the confidentiality, integrity, and availability of business information systems, as well as ensure regulatory compliance and foster greater trust with customers and partners.

Ultimately, the discussion suggests that while the current state of information systems security in Ugandan SEs is full of gaps, the solutions are within reach. With strong management commitment and collective effort guided by a tailored framework, even resource-constrained small enterprises can systematically strengthen their security posture. The standardized yet flexible approach advocated here provides a blueprint for SEs to follow, ensuring that essential security controls and policies are put in place in a way that aligns with their unique needs and limitations. If these recommendations are pursued, small enterprises in Kampala, Wakiso, and similar contexts can greatly improve their resilience against cyber threats, safeguarding their operations and contributing to a more secure digital ecosystem in the long run. The journey to robust information security is iterative and challenging, but by starting with the fundamental steps and building progressively, small enterprises can achieve a level of security that protects their vital assets and sustains their growth in an increasingly information-driven world.

REFERENCES

1, S. K. & Chong, I., 2018. *Correlation Analysis to Identify the Effective Data in Machine Learning: Prediction of Depressive Disorder and Emotion States.* [Online] Available at: https://pmc.ncbi.nlm.nih.gov/articles/PMC6313491/#sec3-ijerph-15-02907 [Accessed 13 2 2025].

27kay, 2023. *The PDCA Cycle: Guide to Implementing it for ISO 27001.* [Online] Available at: https://27kay.com/beginners-guide-to-pdca-for-iso-27001 [Accessed 15 6 2025].

Ahmad, A., Maynard, S. B. & Park, S., 2014. Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing,* 25(2), pp. 1-21.

Al-esaiy, M. A. & Al-Shaibany, D. N. A., 2021. ANALYSIS OF INFORMATION SECURITY MANAGEMENT SYSTEM FRAMEWORKS. *International Journal of Computer Science and Mobile Computing,* 10(11), pp. 29-46.

AlGhamdi, S., Win, K. & Vlahu-Gjorgievska, E., 2020. Information security governance challenges and critical success factors: Systematic review. *Computers & security,* Volume 99.

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

AlHogail, A., 2015. Design and validation of information security culture framework for organizations. *Computer and Information Science,* 8(4), p. 33–41.

Alshboul, Y. & Streff, K., 2015. Analyzing Information Security Model for Small-Medium Sized Businesses. *Americas Conference on Information Systems,* pp. 1-9.

Anwita, 2024. *Types of Security Controls With Examples.* [Online] Available at: https://sprinto.com/blog/types-of-security-controls/#:~:text=these%20in%20steps.-,What%20are%20security%20controls%3F,from%20security%20risks%20or%20threats. [Accessed 6 2 2025].

Arbanas, K. & Hrustek, N. Ž., 2019. Key Success Factors of Information Systems Security. *JIOS,* 43(2), pp. 131-144.

Arya, V., 2022. Cybersecurity for Small and Medium-sized Enterprises (SMEs). *Cyber Security Insights Magazine,* Volume 5.

Ashmead, M., 2023. *The Crucial Role of Senior Management Support in Ensuring an Effective Information Security Program.* [Online] Available at: https://www.linkedin.com/pulse/crucial-role-senior-management-support-ensuring-security-mark-ashmead-rv7uc [Accessed 12 6 2025].

ATLAS.ti, 2024. *The Guide to Interview Analysis.* [Online] Available at: https://atlasti.com/guides/interview-analysis-guide/preparing-a-research-interview [Accessed 21 11 2024].

Authority, U. I., 2025. *SME Portal.* [Online] Available at: https://mybusiness.go.ug/Reports/SMEDirectory?q=Sector&Filters.Enc_SectorId=&Filters.Enc_SubSectorId=&Filters.Enc_GroupId=&Filters.Enc_ClassId=&Filters.SearchTerm=&Filters.Enc_RegionId=&Filters.Enc_SubRegionId=CfDJ8MDfyByZzDROt1XcwmnBuJaVTHO3rd5O_QFSSuHFk [Accessed 23 2 2025].

Balčiūnė, L. & Ramanauskaitė, S., 2019 . Information security management framework suitability estimation for small and medium enterprise. *Technological and Economic Development of Economy,* 25(5), pp. 1-19.

Baskerville, R. et al., 2018. Design Science Research Contributions: Finding a Balance. *Journal of the Association for Information Systems,* 19(5), pp. 358-376.

Bhandari, P., 2020. *Data Collection | Definition, Methods & Examples.* [Online] Available at: https://www.scribbr.com/methodology/data-collection/ [Accessed 4 6 2025].

Bisht, D. R., 2023. *What are Sampling Methods? Techniques, Types, and Examples.* [Online] Available at: https://researcher.life/blog/article/what-are-sampling-methods-techniques-types-and-examples/ [Accessed 19 11 2024].

Blackduck, n.d. *Security Risk Assessment.* [Online] Available at: https://www.blackduck.com/glossary/what-is-security-risk assessment.html#:~:text=A%20security%20risk%20assessment%20identifies,holistically%E2%80%94from%20an%20attacker's%20perspective. [Accessed 4 2 2025].

Bobbert, Y. & Mulder, H., 2015. Governance Practices and Critical Success factors suitable for Business Information Security. *IEEE Computer Society,* pp. 1097-1104.

Bugcrowd, n.d. *CIS Controls Framework (Center for Internet Security).* [Online] Available at: https://www.bugcrowd.com/glossary/cis-controls-framework-center-for-internet-security/#:~:text=The%20CIS%20Framework%20helps%20organizations,implement%20the%20best%20defensive%20mitigations. [Accessed 6 12 2024].

Byjus's, 2024. *Sampling Methods.* [Online] Available at: https://byjus.com/maths/sampling-methods/ [Accessed 19 11 2024].

Carbide, n.d. *How to Use the CIS Controls Framework for Your Business.* [Online] Available at: https://carbidesecure.com/resources/how-to-use-cis-security-framework/ [Accessed 18 12 2024].

Centre, G. C. S. C., 2016. *Cybersecurity Capacity Review of the Republic of Uganda.* 1 ed. Kampala: Global Cyber Security Capacity Centre .

Cisco, n.d. *What Is the NIST Cybersecurity Framework?.* [Online] Available at: And once you have stopped the attack, you need to get back to normal. The Recover function helps you restore operations through recovery planning, continuous improvement, and communications. [Accessed 11 11 2024].

Cleave, P., 2020. *What Is A Good Survey Response Rate?.* [Online] Available at: https://www.smartsurvey.co.uk/blog/what-is-a-good-survey-response rate#:~:text=By%20contrast%2C%20a%20survey%20response,relationship%20between%20the %20business%20and [Accessed 16 4 2025].

Committee, E. A., n.d. *Information System Security Review Methodology,* AUSTRIA: EDP Audit Committee.

community, L., n.d. *What are the most important cybersecurity frameworks for small businesses?.* [Online] Available at: https://www.linkedin.com/advice/0/what-most-important-cybersecurity-frameworks-small-saydf [Accessed 28 1 2025].

Council, T. I., n.d. *Plan- Do – Check – Act ISO 27001.* [Online] Available at: https://isocouncil.com.au/plan-do-check-act-iso 27001/#:~:text=Plan%2D%20Do%20%E2%80%93%20Check%20%E2%80%93%20Act,of%20 the%20ISO%2027001%20standard. [Accessed 13 12 2024].

CSRC, N., n.d. *Computer Security Resource Center.* [Online] Available at: https://csrc.nist.gov/glossary/term/information_systems_security#:~:text=Definitions%3A,docu ment%2C%20and%20counter%20such%20threats. [Accessed 1 22 2025].

CyberArk, n.d. *What is Security Framework?.* [Online] Available at: https://www.cyberark.com/what-is/security-framework/ [Accessed 6 1 2025].

Cymru, B., 2023. *Security Awareness Training for Small Businesses.* [Online] Available at: https://businesswales.gov.wales/news-and-blog/security-awareness-training-small-businesses [Accessed 19 6 2025].

Dawadi, S. S. S. &. G. R. A., 2021. Mixed-Methods Research: A Discussion on its Types, Challenges, and Criticisms. *Journal of Practical Studies in Education,* 2(2), pp. 25-36.

Derek, J. & Kerryn, W., 2023. *Validity & Reliability In Research.* [Online] Available at: https://gradcoach.com/validity-reliability-research/ [Accessed 21 11 2024].

Docs, I., n.d. *COBIT Framework.* [Online] Available at: https://www.itsm-docs.com/blogs/cobit/cobit-framework-pdf [Accessed 06 11 2024].

Drew, J., 2022. *How to Calculate Sample Size for a Survey.* [Online] Available at: https://www.tenato.com/market-research/what-is-the-ideal-sample-size-for-a-survey/ [Accessed 22 2 2025].

Fadhilah, A. R. Y. P. R. a. A. K., 2021. Measurement of information security awareness level: A case study of digital wallet users. In IOP Conference Series: Materials Science and Engineering. 1077(1), p. 12.

FIA, 2024. *Strengthening Cyber Safety and Ransomware Response.* [Online] Available at: https://www.fia.go.ug/strengthening-cyber-safety-and-ransomware-response [Accessed 2 August 2024].

Flowerday, S. & Tuyikeze, T., 2016. Information security policy development and implementation: The what, how and who.. *computers & security,* Volume 61, pp. 169-183.

Flowerday, S. V., 2016. Information security policy development and implementation: The what, how and who. *Computers & Security,* Volume 61, pp. 169-183.

Gashgari, G. W. R. a. W. G., 2017. A Proposed Best-practice Framework for Information Security Governance. *SCITEPRESS – Science and Technology Publications, Lda,* pp. 295-301.

GeeksforGeeks, 2024. *Spearman's Rank Correlation.* [Online] Available at: https://www.geeksforgeeks.org/spearmans-rank-correlation/ [Accessed 14 6 2025].

Gogtay, N. & Thatte, U., 2017. Principles of correlation analysis.. *Journal of the Association of Physicians of India,* 65(3), pp. 78-81.

Governance, I., n.d. *What is Cyber Security? Definition and Best Practices.* [Online] Available at: https://www.itgovernance.co.uk/what-is-cybersecurity [Accessed 15 10 2024].

Grimmick, R., 2024. *What is a Security Policy? Definition, Elements, and Examples.* [Online] Available at: https://www.varonis.com/blog/what-is-a-security-policy [Accessed 26 6 2025].

Group, C., 2024. *PDCA: An implementation guide to ISO 27001:2022.* [Online] Available at: https://citationgroup.com.au/resources/pdca-an-implementation-guide-to-iso-270012022/#:~:text=The%20Plan%2DDo%2DCheck%2D,requirement%20processes%20of%20ISO%2027001. [Accessed 06 11 2024].

Guidance, M. f. I. &. N., 2022. *CYBER SECURITY STRATEGY.* 1 ed. Kampala: Minister for ICT & National Guidance.

Hait, A. W., 2021. *What is a Small Business?.* [Online] Available at: https://www.census.gov/library/stories/2021/01/what-is-a-small-business.html [Accessed 29 1 2025].

Hashemi-Pour, C., 2024. *What is software?.* [Online] Available at: https://www.techtarget.com/searchapparchitecture/definition/software#:~:text=Software%20is%20a%20set%20of,of%20software%20include%20the%20following: [Accessed 27 6 2025].

Holdsworth, J. & Kosinski, M., 2024. *What is information security (InfoSec)?.* [Online] Available at: https://www.ibm.com/think/topics/information-security[Accessed 22 11 2024].

Hørthe, G., 2024. *Balancing In-House & External IT Security: The Hybrid Approach.* [Online] Available at: https://www.nemko.com/blog/it-security-management [Accessed 15 2 2025].

IBM, 2024. *Information Security.* [Online] Available at: https://www.ibm.com/topics/information-security [Accessed 06 11 2024].

ICT, A., 2024. *How CIS v8 & NIS2 Strengthen ISO 27001: A Strategic Synergy.* [Online] Available at: https://alta-ict.nl/en/blog/how-cis-v8-can-complement-iso-27001-a-strategic-approach/ [Accessed 18 12 2024].

Imperva, n.d. *Information Security: The Ultimate Guide.* [Online] Available at: https://www.imperva.com/learn/data-security/information-security infosec/#:~:text=of%20Digital%20Transformation.,What%20are%20the%203%20Principles%20of%20Information%20Security%3F,are%20called%20the%20CIA%20Triad. [Accessed 23 1 2025].

infrastructure.go.ug, 2024. *Progress on ICT.* [Online] Available at: https://infrastructure.go.ug/progress-on-information-and-communication/ [Accessed 15 July 2024].

Kabir, S. M. S., 2016. METHODS OF DATA COLLECTION. In: *Basic Guidelines for Research.* s.l.:s.n., pp. 201-275.

Kayworth, T. & Whitten, D., 2016. Effective information security requires a balance of social and technical factors. *MIS Quarterly Executive,,* 5(3), p. 163–175.

Kelly, D. & Luo, X. W., 2003. *Data Collection Procedure.* [Online] Available at: https://www.sciencedirect.com/topics/computer-science/data-collection-procedure [Accessed 21 11 2024].

Kerner, S. M., 2025. *What is continuous monitoring?.* [Online] Available at: https://www.techtarget.com/searchitoperations/definition/continuous-monitoring [Accessed 10 5 2025].

Kimwele, M. M. W. a. K. S., 2011. Information technology (IT) security framework for Kenyan small and medium enterprises (SMEs). *International Journal of Computer Science and Security ,* 5(1), p. 39.

Kirvan, P., 2023. *Top 12 IT security frameworks and standards explained.* [Online] Available at: https://www.techtarget.com/searchsecurity/tip/IT-security-frameworks-and-standards-Choosing-the-right-one [Accessed 11 12 2024].

Koskosas, I. & Giaglis, G., 2022. Information security management in SMEs: Challenges and opportunities. *Journal of Small Business and Enterprise Development,* 29(1), p. 57–76.

Lanter, D. D., 2018. *COBIT® 2019 Framework.* 50 ed. s.l.:ISACA.

Lazaar, Y., 2024. *Design Science Research Methodology.* [Online] Available at: https://medium.com/@yassin.lazar/design-science-research-methodology-4577f732a1fa [Accessed 12 1 2025].

Leger, B., 2024. *11 Information Security Strategies for Your Business.* [Online] Available at: https://infotech.us/strategies-for-information-security/ [Accessed 15 1 2025].

Limited, S., 2020. *Africa Cybersecurity Report,* Kampala: Serianu Limited.

Liontos, G., Katsouras, A., Liagkou, V. & Glavas, E., 2025. Cybersecurity Guide for SMEs: Protecting Small and Medium-Sized Enterprises in the Digital Era. *Journal of Information Security,* 16(1), pp. 1-43.

Manjezi, Z. & Botha, R., 2019. From concept to practice: untangling the direct-control cycle. *International Conference on Information Communication and Management ,* pp. 101-105.

Mário Antunes, M. M. R. G. D. P., 2021. Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. *Journal of Cybersecurity and Privacy,* 1(2), p. 219–238.

Maslakci, A., Sürücü, L. & Yikilmaz, İ., 2022. Exploratory Factor Analysis (EFA) in Quantitative Researches and Practical Considerations. *Gümüşhane Üniversitesi Sağlık Bilimleri Dergisi,* 13(2), pp. 947-965.

McGrath, A. & Jonker, A., 2025. *What is risk management?.* [Online] Available at: https://www.ibm.com/think/topics/riskmanagement#:~:text=Risk%20management%20is%20the%20process,errors%2C%20accidents%20and%20natural%20disasters. [Accessed 10 4 2025].

Melaku, H., 2023. A Dynamic and Adaptive Cybersecurity Governance Framework. *Journal of Cybersecurity and Privacy,* 3(3), pp. 327-350.

Mirtsch, M., Kinne, J. & Blind, K., 2021. Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis. *IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT,* 68(1), pp. 87-100.

Moffat, A., n.d. *CIS Controls.* [Online] Available at: https://www.sapphire.net/blogs-press-releases/cis-controls/ [Accessed 11 12 2024].

Mukherjee, S., 2022. *What is Information System? Definition, Examples, & Facts.* [Online] Available at: https://emeritus.org/in/learn/information-system/ [Accessed 27 6 2025].

Mustakim, S. S., Atmoko, A., Hanafi, Y. & Nusantoro, T., 2023. Module Validation via Delphi Techniques: One Consensus and Unanimity. *Open Access Journal,* 12(4).

Mwanje, D., Samuel, O., Tumwebaze, G. & Bukenya, M., 2023. A Framework to Enhance Information Security Governance in SMEs. *Saudi Journal of Engineering and Technology,* pp. 300 -303.

Myers, M. D., n.d. Qualitative Research in Information Systems. *MIS Quarterly,* Issue 249422, pp. 1-19.

Nationwide, n.d. *Risk management for small businesses.* [Online] Available at: https://www.nationwide.com/business/solutions-center/risk-management/risk-management-for-small business#:~:text=A%20risk%20management%20strategy%2C%20then,not%20all%20risks%20are%20negative. [Accessed 19 6 2025].

Nature, S., 2024. *Study Population.* [Online] Available at: https://link.springer.com/referenceworkentry/10.1007/978-94-007-0753-5_2893 [Accessed 19 11 2024].

NITA-U, 2014. *National Infomation Security Framework.* [Online] Available at: https://www.nita.go.ug/sites/default/files/202201/National%20Information%20Security%20Policy%20v1.0_0.pdf [Accessed 11 12 2024].

Novriansyah, N., 2024. *Understanding Information Security Strategy: What, Why, Who, How.* [Online] Available at: https://medium.com/novai-cism-101/understanding-information-security-strategy-what-why-who-how-bf645099131e [Accessed 8 2 2025].

nqa, n.d. *ISO 27001:2022 INFORMATION SECURITY IMPLEMENTATION GUIDE.* s.l.:s.n.

Otero, A., 2015. An information security control assessment methodology for organizations' financial information. *International Journal of Accounting Information Systems,* Volume 18, pp. 26-45..

Otucu, F., 2024. *Gov't Attributes Rise in Cyber Attacks to 4.5% Growth in ICT Sector.* [Online] Available at: https://chimpreports.com/govt-attributes-rise-in-cyber-attacks-to-4-5-growth-in-ict-sector/ [Accessed 29 1 2025].

Packetlabs, 2024. *A Guide to Fundamental Security Control Types.* [Online] Available at: https://www.packetlabs.net/posts/a-guide-to-fundamental-security-control-types/ [Accessed 24 1 2025].

Palatty, N. J., 2025. *51 Small Business Cyber Attack Statistics 2025 (And What You Can Do About Them).* [Online] Available at: https://www.getastra.com/blog/security-audit/small-business-cyber-attackstatistics/#:~:text=Overview%20Of%20Small%20Business%20Cyber%20Attacks&text=face%20cyber%20attacks.,Accenture's%20Cybercrime%20Study%20reveals%20that%20nearly%2043%25%20of%20cyber%2 [Accessed 19 6 2025].

Papathanasiou, A., Liontos, G., Liagkou, V. & Glavas, E., 2024. Enhancing Information Security for Businesses and Organizations: Practical Controls and Systems Frameworks. *SCIREA Journal of Information Science and Systems Science,* 8(4), pp. 154-173.

Paulsen, C. & Toth, P., 2016. *Small Business Information Security: The Fundamentals,* Gaithersburg: National Institute of Standards and Technology .

PECB, n.d. *ISO/IEC 27001 Information Security Management System.* [Online] Available at: https://pecb.com/en/education-and-certification-for-individuals/iso-iec-27001 [Accessed 06 11 2024].

Poitier, F., 2024. Developing a Structured Approach to Document Reviews: Lessons from a qualitative study in The Bahamas. Issue 9781529684407, pp. 1-27.

Publishing, I. G. S., 2013. Experiences in Applying Mixed-Methods Approach in Information Systems Research. *Experiences in Applying Mixed-Methods Approach in Information Systems Research,* p. 28.

Rapid7, 2024. *Information Security Risk Management.* [Online] Available at: https://www.rapid7.com/fundamentals/information-security-riskmanagement/#:~:text=Information%20security%20risk%20management%2C%20or,availability%20of%20an%20organization's%20assets [Accessed 5 12 2024].

Reis, L. M. C. a. W. T., 2022. Mixed-Methods in Information Systems Research: Status Quo, Core Concepts, and Future Research Implications. *Communications of the Association for Information Systems,* 51(1), p. 17.

Renaud, K. & Goucher, W., 2021. p. 172.

Safa, N., Von Solms, R. & Furnell, S., 2016. Information security policy compliance model in organizations. *Computers & Security,* Volume 56, p. 70–82.

Sataloff, R. & Vontela, S., 2021. Response Rates in Survey Research. *Journal of Voice,* 35(10).

ScienceDirect, 2015. *Research Ethics.* [Online] Available at: https://www.sciencedirect.com/topics/social-sciences/research-ethics [Accessed 22 11 2024].

SecurDI, 2023. *The Importance of Cybersecurity Frameworks for Small and Medium-Sized Enterprises.* [Online] Available at: https://securdi.com/cyber-security/the-importance-of-cybersecurity-frameworks-for-small-and-medium-sized-enterprises/ [Accessed 11 12 2024].

Senthilnathan, S., 2019. Usefulness of correlation analysis. *SSRN* .

Sharma, A. & Dash, S., 2020. Cybersecurity challenges in SMEs: A case study of Indian enterprises'. *International Journal of Information Management,* Volume 53, p. 1–10.

Sharma, S. & Sugumaran, V., 2011. A Framework for Enhancing Systems Security. *Journal of Information Privacy & Security,* 7(4), pp. 3-22.

Technology, N. I. o. S. a., 2024. The NIST Cybersecurity Framework (CSF) 2.0. In: s.l.:s.n., pp. 1-32.

Technology, N. I. o. S. a., 2024. *The NIST Cybersecurity Framework (CSF) 2.0.* [Online] Available at: https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final [Accessed 21 2 2025].

Tornberg, P., n.d. *Seadot Cybersecurity.* [Online] Available at: https://seadot.se/en/cybersecurity/security-frameworks/ [Accessed 4 12 2024].

To, S. H., n.d. *Kaiser-Meyer-Olkin (KMO) Test for Sampling Adequacy.* [Online] Available at: https://www.statisticshowto.com/kaiser-meyer-olkin/ [Accessed 8 2 2025].

Tuhin, M., 2025. *Why Cybersecurity Will Be More Important Than Ever in 2025.* [Online] Available at: https://www.sciencenewstoday.org/why-cybersecurity-will-be-more-important-than-ever-in-2025 [Accessed 12 6 2025].

UIA, n.d. *Domestic Investment.* [Online] Available at: https://www.ugandainvest.go.ug/sme/ [Accessed 6 1 2025].

University, N., n.d. *Strength of Correlation.* [Online] Available at: https://www.ncl.ac.uk/webtemplate/ask-assets/external/maths-resources/statistics/regression-and-correlation/strength-of correlation.html#:~:text=Pearson's%20Product%20Moment%20Correlation%20Coefficient,monotonic%20correlation%20between%20two%20variables. [Accessed 13 2 2025].

Vahid, Z., Akram, G., Maryam, R. & Abbas, A., 2015. Design and Implementation Content Validity Study: Development of an instrument for measuring Patient-Centered Communication. *Journal of Caring Sciences,* 4(10.15171), pp. 166-175.

Vicente, V., 2024. *Step-by-Step Internal Audit Checklist.* [Online] Available at: https://auditboard.com/blog/audit-checklist-how-to-conduct-an-audit-step-by-step [Accessed 10 6 2025].

Von Solms, R. a. v. S. S., 2006. Information Security Governance: a model based on the direct–control cycle. *Computers & security,* 25(6), pp. 408-412.

Wadhwa, P., 2024. *Cybersecurity for Small Businesses.* [Online] Available at: https://sprinto.com/blog/cybersecurity-for-small-businesses/ [Accessed 29 4 2025].

Wadie, R. & Ahuja, H., 2025. *RSM International Ltd.* [Online] Available at: https://www.rsm.global/insights/how-much-will-data-breach-cost-you [Accessed 10 4 2025].

Whitman, M. E., 2018. Security Education, Training, and Awareness Program. In: *Principles of Information security.* Boston: Cengage Learning, pp. 211 - 214.

Whitman, M. E. & Herbert J. Mattord, 2018. *Principles of Information Security.* 6 ed. Boston: Cengage Learning.

Writer, B. T., 2024. *How Can Cybersecurity be Enhanced in Uganda's Evolving Cashless Economy?.* [Online] Available at: https://businesstimesug.com/how-can-cybersecurity-be-enhanced-in-ugandas-evolving-cashless-economy/ [Accessed 29 1 2025].

Yazan, A. & Kevin, S., 2015. *Analyzing Information Security Model for Small-Medium Sized Businesses.* Puerto Rico, Twenty-first Americas Conference on Information Systems.

Zanke, A., Weber, T., Dornheim, P. & Engel, M., 2024. *Assessing information security culture: A mixed-methods approach to navigating challenges in international corporate IT departments. Computers & Security.* [Online] Available at: https://www.sciencedirect.com/science/article/abs/pii/S0167404824002438 [Accessed 19 11 2024].

Zemmouchi-Ghomari, L., 2021. Basic Concepts of informationsystems. *Contemporary Issues in Information Systems-A Global Perspective..*

Zwass, V., 2025. *information system.* [Online] Available at: https://www.britannica.com/topic/information-system/Information-systems-in-the-economy-and-society [Accessed 27 6 2025].

Sharma, Srinarayan & Sugumaran, Vijayan. (2011). A Framework for Enhancing Systems Security. Journal of Information Privacy and Security. 7. 3-22.10.1080/15536548.2011.10855921.

APPENDICES

Appendix 1: Data Collection Introductory Letter

Uganda Martyrs University

making a difference

OFFICE OF THE DEAN, FACULTY OF SCIENCE
Email:deanscience@umu.ac.ug

Date: 2nd April 2025

To Whom it May Concern.

Dear Sir/Madam,

Re: Assistance for Research – Mr. MUSINGUZI Jimmy (2023-M132-21504)

Greetings from the Faculty of Science, Uganda Martyrs University.

This is to introduce to you **Mr. MUSINGUZI Jimmy** registration Number; **2023 - M132-21504**, a final year student pursuing a Master of Science Degree in Information Systems. He is carrying out a research on the topic: ***"Framework for Enhancing Information Systems Security among Small Enterprises in Uganda,"***as part of the curriculum requirements for the award of a master's Degree of this University.

I kindly, request you to render him such assistance as may be necessary for the research.

I hope that his application will receive your favourable consideration.

Any assistance rendered to him will be highly appreciated.

Please do not hesitate to contact our office for any further information.

Yours faithfully,

Rev. Fr. Henry Nsubuga Kiwanuka (PhD)
DEAN.

Uganda Martyrs University 02 APR 2025 FACULTY OF SCIENCE

Uganda Martyrs University P.O. Box 5498 – Kampala - Uganda
Tel: (+256)382 – 410 611 Fax: (+256)382 – 410 100 Email: umu@umu.ac.ug

Appendix 2: Survey Questionnaire

QUESTIONNAIRE: ENHANCING INFORMATION SYSTEMS SECURITY AMONG SMALL ENTERPRISES IN UGANDA

Dear Respondent,

My name is Jimmy Musinguzi a post graduate student at Uganda Martyrs University currently pursuing a Master of Science in Information Systems. I am currently conducting research titled ″A Framework for Enhancing Information Systems Security among Small Enterprises in Uganda″

The main objective of this survey is to establish requirements for the design of a framework to enhance information systems security among small enterprises in Uganda. The research is purely academic, confidential and will be solely used for that purpose. Therefore, I would request you to take a few moments of your time to answer the following few questions. Thank you very much for your cooperation.

CONSENT: Do you allow me to proceed? Yes ☐ No ☐

SECTION A: BACKGROUND INFORMATION

1. Name of Enterprise: _____
2. Position in the Enterprise:
   - ☐ IT Professional
   - ☐ Manager
   - ☐ Executive
3. How many employees does your enterprise have?
   - ☐ 1-10
   - ☐ 11-20
   - ☐ 21-50
4. What is your enterprise's annual revenue (UGX)?
   - ☐ Below 100 million
   - ☐ 100-200 million

- ☐ 201-360 million

5. How long has your enterprise been in operation?
   - ☐ Less than 1 year
   - ☐ 1-3 years
   - ☐ 4-6 years
   - ☐ More than 6 years

SECTION B: EXISTING INFORMATION SECURITY FRAMEWORKS & REQUIREMENTS

Directions: Below is a list of statements. Tick in the spaces provided at the end of the questions

6. Our enterprise has a formal information security policy in place.
   - ☐ Strongly Agree
   - ☐ Agree
   - ☐ Neutral
   - ☐ Disagree
   - ☐ Strongly Disagree
7. We follow a recognized information security framework (e.g., ISO 27001, NIST, etc.).
   - ☐ Strongly Agree
   - ☐ Agree
   - ☐ Neutral
   - ☐ Disagree
   - ☐ Strongly Disagree
8. The existing security framework meets the specific needs of our small enterprise.
   - ☐ Strongly Agree
   - ☐ Agree
   - ☐ Neutral
   - ☐ Disagree

- ☐ Strongly Disagree

9. What are the biggest information security challenges your enterprise faces? (Select all that apply)
   - ☐ Limited budget for cybersecurity
   - ☐ Lack of expertise in cybersecurity
   - ☐ Lack of awareness among employees
   - ☐ Weak policies and procedures
   - ☐ Increased cyber threats and attacks

SECTION C: DESIGNING A SECURITY FRAMEWORK FOR SEs

10. Our enterprise has experienced security breaches or cyber threats in the past year.
    - ☐ Strongly Agree
    - ☐ Agree
    - ☐ Neutral
    - ☐ Disagree
    - ☐ Strongly Disagree
11. Our enterprise regularly updates its security policies and software.
    - ☐ Strongly Agree
    - ☐ Agree
    - ☐ Neutral
    - ☐ Disagree
    - ☐ Strongly Disagree
12. Data encryption and access control measures are in place to protect sensitive information.
    - ☐ Strongly Agree
    - ☐ Agree
    - ☐ Neutral
    - ☐ Disagree

- ☐ Strongly Disagree

13. Our company provides regular cybersecurity training to employees.
    - ☐ Strongly Agree
    - ☐ Agree
    - ☐ Neutral
    - ☐ Disagree
    - ☐ Strongly Disagree
14. What security measures does your enterprise currently have in place? (Select all that apply)
    - ☐ Firewalls and antivirus software
    - ☐ Regular data backups
    - ☐ Secure passwords and authentication methods
    - ☐ Network monitoring tools
15. Non – disclosure agreements (NDAs) are signed with all third-party IT vendors before executing any IT service.
    - ☐ Strongly Agree
    - ☐ Agree
    - ☐ Neutral
    - ☐ Disagree
    - ☐ Strongly Disagree
16. Background checks are done on all IT vendors before onboarding them.
    - ☐ Strongly Agree
    - ☐ Agree
    - ☐ Neutral
    - ☐ Disagree
    - ☐ Strongly Disagree

17. The company conducts risk assessment to identify the key objectives that need to be supported by the information systems security program.

    - ☐ Strongly Agree
    - ☐ Agree
    - ☐ Neutral
    - ☐ Disagree
    - ☐ Strongly Disagree

18. Outsourced software development is supervised and monitored.

    - ☐ Strongly Agree
    - ☐ Agree
    - ☐ Neutral
    - ☐ Disagree
    - ☐ Strongly Disagree

19. All business-critical applications are reviewed and tested after changes to operating system platforms and changes to software packages are restricted.

    - ☐ Strongly Agree
    - ☐ Agree
    - ☐ Neutral
    - ☐ Disagree
    - ☐ Strongly Disagree

20. There are mechanisms for identifying information systems security threats and vulnerabilities associated with each of the critical assets and functions.

    - ☐ Strongly Agree
    - ☐ Agree
    - ☐ Neutral
    - ☐ Disagree
    - ☐ Strongly Disagree

21. The company has a documented User Acceptance Policy which is signed by all new employees.

    - ☐ Strongly Agree
    - ☐ Agree
    - ☐ Neutral
    - ☐ Disagree
    - ☐ Strongly Disagree

22. There is a documented information security strategy that is updated from time to time in line with company objectives.

    - ☐ Strongly Agree
    - ☐ Agree
    - ☐ Neutral
    - ☐ Disagree
    - ☐ Strongly Disagree

23. Management plays a great role in enforcing information systems security awareness trainings among employees.

    - ☐ Strongly Agree
    - ☐ Agree
    - ☐ Neutral
    - ☐ Disagree
    - ☐ Strongly Disagree

SECTION D: VALIDATION OF THE FRAMEWORK

24. An information security framework tailored to small enterprises is necessary.

    - ☐ Strongly Agree
    - ☐ Agree
    - ☐ Neutral

- ☐ Disagree
- ☐ Strongly Disagree

25. Our enterprise would adopt a standardized information security framework if provided.
    - ☐ Strongly Agree
    - ☐ Agree
    - ☐ Neutral
    - ☐ Disagree
    - ☐ Strongly Disagree
26. External audits and security assessments help improve our information security measures.
    - ☐ Strongly Agree
    - ☐ Agree
    - ☐ Neutral
    - ☐ Disagree
    - ☐ Strongly Disagree
27. What additional recommendations do you have for improving information systems security in SEs?

    ……
    ……
    ……
    ……

Thank you so much for your participation

Appendix 3: Thematic Analysis

Theme 1: Background Information

Sub-theme: Nature and Size of Enterprise

- Enterprises ranged from 5 to 50 employees, with most operational for 3–10 years.
- Majority were tech start-ups, retail businesses, or service-based SEs.

Sub-theme: Role of Respondents

- Most respondents were founders, co-founders, operations managers, or IT heads.

Sub-theme: Perception of Information Security

- *"Information security is vital for maintaining customer trust and safeguarding data. Without it, our credibility is at risk."* – Founder, Logistics SE, Kampala

Theme 2: Existing Information Security Frameworks & Requirements

Sub-theme: Presence of Formal Security Policies

- Many had informal or outdated policies, with few having structured documentation.

"We understand the risks, but developing a comprehensive policy requires expertise and time, which we just don't have in-house." – Business Owner, Technology Enterprise, Kampala

Sub-theme: Use of Recognized Frameworks

- ISO 27001 or NIST frameworks were rarely implemented directly.

"Most frameworks like ISO 27001 are built with larger organizations in mind. We have to adapt them significantly to make them workable for our scale." – IT Manager, Retail Business, Wakiso

Sub-theme: Cyber Threat Experiences

- 11 of 20 businesses had experienced phishing, malware, or unauthorized access in the past year.

"We're constantly on the lookout for new threats, but the budget we have just doesn't stretch far enough... It's a constant battle to stay protected." – IT Manager, Retail Business, Wakiso

Sub-theme: Frequency of Policy/Software Updates

- Updates were done on an ad-hoc basis. Formal review cycles were rare.

Sub-theme: Key Security Challenges

- Limited staff expertise, minimal budgets, and employee awareness were cited most.

"The biggest challenge we face is not just having security policies, but making sure everyone from top management to junior staff actually understands and follows them." – Manager, IT Firm, Kampala

Theme 3: Security Controls

Sub-theme: Authentication & Access Control

- Majority used strong passwords; few had multi-factor authentication or role-based access control systems.

Sub-theme: Security Tools

- Firewalls and antivirus were the most used tools.

"We rely on antivirus and firewalls, but we don't do things like risk assessments or background checks on IT vendors. To be honest, we haven't formalized our security framework — it is mostly reactive. – Operations Manager, Retail Enterprise, Wakiso

Sub-theme: Secure Data Handling

- Encryption and secure transmission protocols were not consistently applied.

Sub-theme: Employee Offboarding

- Commonly lacked proper access revocation processes.

Theme 4: Risk Management

Sub-theme: Risk Assessments

- Few businesses conducted formal assessments; most relied on intuition or reactive measures.

Sub-theme: Backup and Recovery

- Cloud storage and manual external drives were commonly used, few tested recovery readiness.

Sub-theme: Vendor Security Evaluation

- Background checks and compliance reviews were rare.

Sub-theme: System Updates

- Most updates were performed only when prompted by software.

Sub-theme: Outsourced Development

- Freelance or third-party developers used without consistent security vetting.

Theme 5: Validation of the Security Framework

Sub-theme: Need for Tailored Frameworks

- All participants emphasized the necessity of a SE-focused security framework.

"Cybersecurity frameworks built for corporate giants don't work for us. We need something lightweight and adaptable." – Co-founder, Agritech Startup, Wakiso

Sub-theme: Willingness to Adopt a Standard Framework

- High willingness if the framework is low-cost, easy to understand, and comes with local support.

Sub-theme: Influence of Audits

- External audits were rare but viewed as potentially helpful.

Sub-theme: Recommendations

- Calls for:
  - ✓ Localized, practical frameworks
  - ✓ Subsidized cybersecurity training
  - ✓ Public-private partnerships
  - ✓ Clear communication of policies within SEs

Appendix 4: Framework Evaluation Questionnaire

A Framework for Enhancing Information Systems Security Among Small Enterprises in Uganda

Evaluation Questionnaire

Dear Respondent,

My name is Jimmy Musinguzi a post graduate student at Uganda Martyrs University currently pursuing a Master of Science in Information Systems. I am currently evaluating my designed framework titled ″A Framework for Enhancing Information Systems Security among Small Enterprises in Uganda″

The purpose of this survey is to establish if the designed framework is practical, straightforward and applies low-cost measures suitable for such resource-constrained businesses. The research is purely academic, confidential and will be solely used for that purpose. Therefore, I would request you to take a few moments of your time to answer the following few questions. Thank you very much for your cooperation.

Instructions: For each statement below, please indicate how much you agree or disagree, using the scale 1 (Strongly Disagree) to 5 (Strongly Agree).

a) Relevance

1. The framework caters for the specific information security needs of small enterprises like ours.
   - ☐ Strongly Agree
   - ☐ Agree
   - ☐ Neutral
   - ☐ Disagree
   - ☐ Strongly Disagree
2. The framework can address the information security of small enterprises which are constrained on resources.
   - ☐ Strongly Agree
   - ☐ Agree
   - ☐ Neutral
   - ☐ Disagree
   - ☐ Strongly Disagree

3. The framework is suitable for the small business environment and regulatory context in Uganda.
    - ☐ Strongly Agree
    - ☐ Agree
    - ☐ Neutral
    - ☐ Disagree
    - ☐ Strongly Disagree
4. The artifact explores the main security challenges encountered by our enterprise.
    - ☐ Strongly Agree
    - ☐ Agree
    - ☐ Neutral
    - ☐ Disagree
    - ☐ Strongly Disagree
5. The guidelines and instructions within the framework are concise and applicable to our enterprise.
    - ☐ Strongly Agree
    - ☐ Agree
    - ☐ Neutral
    - ☐ Disagree
    - ☐ Strongly Disagree

b) Usability

6. The framework is easy to well-organized and easy to understand.
    - ☐ Strongly Agree
    - ☐ Agree
    - ☐ Neutral
    - ☐ Disagree
    - ☐ Strongly Disagree
7. The processes and steps of the framework are easy to follow.
    - ☐ Strongly Agree
    - ☐ Agree
    - ☐ Neutral
    - ☐ Disagree
    - ☐ Strongly Disagree

8. Our company's non-technical employees can utilize the framework with ease.

- ☐ Strongly Agree
- ☐ Agree
- ☐ Neutral
- ☐ Disagree
- ☐ Strongly Disagree

9. The template can be utilized without consuming too much of our team's time or effort.

- ☐ Strongly Agree
- ☐ Agree
- ☐ Neutral
- ☐ Disagree
- ☐ Strongly Disagree

c) Effectiveness

10. The framework helps deal with important information security problems, like data breaches and phishing.

- ☐ Strongly Agree
- ☐ Agree
- ☐ Neutral
- ☐ Disagree
- ☐ Strongly Disagree

11. Applying the framework would probably enhance our enterprise's general security stance.

- ☐ Strongly Agree
- ☐ Agree
- ☐ Neutral
- ☐ Disagree
- ☐ Strongly Disagree

12. The best practices and security controls suggested by the framework are adequate to keep our data safe.

- ☐ Strongly Agree
- ☐ Agree
- ☐ Neutral
- ☐ Disagree

- [ ] Strongly Disagree

13. The framework offers extensive coverage of security practices that are required.

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

14. We believe this framework would be ideal in mitigating cyber-attacks on our enterprise.

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