DEPARTMENT OF COMPUTER AND INFORMATION SCIENCES

Information Security Policies for Digitised Identity Systems: An Investigation into the Views of Stakeholders of the Ghanaian National Identity System

A Thesis Presented to the Department of Computer and Information Sciences

By

SALIM AWUDU

In Partial Fulfilment of the Requirements for the Degree of Doctor of Philosophy in Computer and Information Sciences

June 15, 2025

‘This thesis is the result of the author’s original research. It has been composed by the author and has not been previously submitted for examination which has led to the award of a degree.’ 'The copyright of this thesis belongs to the author under the terms of the United Kingdom Copyright Acts as qualified by University of Strathclyde Regulation 3.50. Due acknowledgement must always be made of the use of any material contained in, or derived from, this thesis.’

Signed: Salim Awudu

Date: December 15, 2025

Dedication

This thesis is dedicated to:

- My mum, Madam Ayishatu Basiru Awudu and my uncle, Alhaji Rauph Awudu Iddrisu, for their inspiration and belief in me. Their selfless financial support aided me in my academic journey.
- My siblings, Nafisah, Zakiyya, Masali and Basiru (who passed on), I am grateful for your love, and motivation.
- To Melica Lee, your companionship and understanding have been invaluable to this journey.
- And to my friends, mentors and advisors, I am grateful for your counsel, and support.

I am grateful to all those who supported me in one way or the other.

This thesis is evidence of your faith support and encouragement.

Acknowledgement

This thesis has materialised based on the assistance and encouragement of some lovely people and I acknowledge that without their advice and support, I could not have achieved it.

First, I am eternally grateful to my supervisor, Dr Sotirios Terzis for his guidance, trust and priceless support in this journey. Dr Sotirios provided the necessary direction, feedback, and valuable input to this thesis. I am immensely thankful for helping me benefit from his research knowledge and skills.

I also acknowledge the University of Strathclyde for considering and selecting me as a scholar of the PGR awards, providing an enabling learning environment and the tools to carry out this academic work.

To some bosses and friends like Mr Samuel Afari Dartey, Mrs Betty Mould Iddrisu, Mr Josef Iroko ESQ, Osei Kwame Griffiths, Prof Kwamina Ahwoi and all others, and my family, I am eternally grateful.

I am also grateful to all heads and participants from all participating institutions in this research. Special thanks go to Prof Kenneth Agyemang Attafuah, the NIA Executive Secretary, the CEOs of the participating institutions and fellow PhD research students for their various roles in this research work.

Last but not least, I am grateful to scholars, authors and organisations whose work became inputs or contributions to my research thesis. Their contributions became the foundation upon which I built upon to put this thesis together and I am fully responsible for any mistakes or omissions in this thesis.

Salim Awudu

June 15, 2025

Abstract

The increasing adoption of Electronic Identity Systems (EIS) globally has transformed identity management and verification processes enhancing efficiency in public service delivery. Information Security Policies (ISPs) play an important role in ensuring data security and privacy in all information systems. However, the specific ISP needs of EIS particularly in developing countries, have received little attention to date.

The aim of this thesis is to understand the ISP needs of EIS with a focus on development countries, using the Ghanaian National Identification Authority (NIA) EIS as a case study. The thesis investigates the formulation, development, implementation, and evolution of the NIA's ISP from the perspective of its stakeholders, NIA staff, user agencies and the public.

The findings reveal that while NIA staff acknowledge the importance of the ISP, there is limited stakeholder involvement and communication during its development. External stakeholders express varying levels of trust and engagement and call for clearer responsibilities and greater transparency in security practices. The study highlights the need to formalise policy development processes, align them with government regulations, and involve both public and private sector experts. It also identifies a gap between public expectations and the NIA's engagement efforts, underscoring the importance of transparency and proactive communication in building trust.

This research contributes to the field by offering practical recommendations for improving ISP communication, stakeholder engagement, and overall information security management. It emphasises the need for EIS organisations to regularly review and update their ISPs with stakeholder input to enhance compliance, effectiveness, and public trust in digital identity systems.

Publication

Awudu, S., & Terzis, S. (2021, September). Information Security Policy Awareness Beliefs versus Reality in Electronic Identity Systems: A Case Study of the Ghanaian National Identity System”. A poster presentation at SICSA Conference hosted by University of Dundee, United Kingdom.

Awudu, S., & Terzis, S. (2022, November). Information security policy awareness beliefs versus reality in electronic identity systems: A case study of the Ghanaian National Identity System. In The Sixteenth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies. Retrieved from https://www.thinkmind.org/articles/digital_2022_2_20_20014.pdf.

Awudu, S., & Terzis, S. (2023, March). INVESTIGATING STAFF INFORMATION SECURITY POLICY COMPLIANCE IN ELECTRONIC IDENTITY SYSTEMS–THE GHANAIAN NATIONAL IDENTITY SYSTEM. In International Conference for International Association for Development of the Information Society (IADIS): Proceedings of International Conferences e-society and Mobile Learning (pp. 68-75).

Awudu, S., & Terzis, S. (2024, July). Information Security Management in Digitized Identity Systems: The Case of the Ghanaian National Identification Authority (NIA). In International Symposium on Human Aspects of Information Security and Assurance (pp. 134-147). Cham: Springer Nature Switzerland.

Contents

List of Figures

List of Tables

List of Abbreviations

ADB: Agricultural Development Bank

APA: American Psychological Association

AU: African Union

BDR: Birth and Death Registry

CAQDAS: Computer-Assisted Qualitative Data Analysis Software

CARE: Collective Benefits, Authority to Control, Responsibility Ethics

CAGD: Controller and Accountant Generals' Department

CCPA: California Consumer Privacy Act

CCTV: Closed-Circuit Television

CEO: Chief Executive Officer

CFO: Chief Finance Officer

CIA: Confidentiality, Integrity and Availability

CIDR: Central Identity Repository

CIO: Chief Information Officer

CISA: Certified Information Systems Auditor

CIS: Computer and Information Science

CISO: Chief Information Security Officer

DVLA: Drivers and Vehicle Licensing Authority

eID: Electronic Identity

EIS: Electronic Identity Systems

EIS ISP: Electronic Identity Systems Information Security Policy

EU: European Union

EU DPD: European Union Data Protection Directive

EVM: Electronic Voting machine

FAIR: Findable, Accessible, Interoperable, and Reusable

GCB: Ghana Commercial Bank

GDPR: General Data Protection Regulation

GIA-ISP: Ghanaian Identification Authority Information Security Policy

GIS: Ghana Immigration Service

GNIS: Ghanaian National Identity System

GPS: Ghana Police Service

GRA: Ghana Revenue Authority

HIPAA: Health Insurance Portability and Accountability Act

HR: Human Resources

IATRP: Information Assurance Training and Ratings Program

ICT: Information and Communication Technology

ID: Identity

IMS: Integrated Margins Group

IS: Information Security

ISACA: Information Systems Audit and Control Association

ISMS: Information Security Management Systems

ISO: International Organisation for Standardisation

ISP: Information Security Policy

ISM: Information Security Management

ISA: Information Systems Authority

IT: Information Technology

L.I: Legislative Instrument

MDA: Ministries, Departments or Agencies

MIS: Management Information System

MOU: Memorandum of Understanding

NHIA: National Health Insurance Authority

NHIS: National Health Insurance System

NIA: National Identification Authority

NIA ISP: National Identification Authority Information Security Policy

NIS: National Identification System

NITA: National Information and Technology Agency

NUDIST: Non-numerical Unstructured Data Indexing, Searching, and Theorising

PCI DSS: Payment Card Industry Data Security Standard

PIPEDA: Personal Information Protection and Electronic Documents Act (PIPEDA)

PPME: Planning, Monitoring and Evaluation

PwC: PricewaterhouseCoopers

RIHA: Riigi Infosüsteemi Halduse Infosüsteem (state information systems and data)

RITE: Responsibility, Integrity, Trust and Ethicality

SDG: Sustainable Development Goal

SIM: Subscriber Identity Module

SOP: Standard Operating Procedure

SOX: Sarbanes–Oxley Act

SPSS: Statistical Package for the Social Sciences

SSI: Self-Sovereign Identity

SSNIT: Social Security and National Insurance Trust

TIN: Tax Identification Number

UIDAI: Unique Identification Authority of India

1 Research Introduction

This chapter provides an overview of the research, including the motivation behind the study, the research problems and questions, the methodological approach, the research outcomes, contributions, and the dissertation outline.

1.1 Motivation

The emergence of electronic identity systems (EIS) globally has revolutionised how identities are managed and verified. Systems such as the Estonian Digital Identity System and India's Aadhaar System have demonstrated the critical role these systems play in facilitating secure and efficient service delivery (Robles-Carrillo, 2024; Glöckler, et.al, 2023). The importance of information security in these systems cannot be overstated, as they handle sensitive personal data and are prime targets for attacks (Anand & Brass, 2021). Information security policies (ISPs) are crucial in ensuring the security and trustworthiness of these systems (Flowerday & Tuyikeze, 2016). This research aims to address the gap in the literature regarding the specific challenges and requirements of ISPs in EIS, using the Ghanaian National Identification Authority (NIA) as a case study. It also aims to identify and address the specific ISP development, implementation and evolution challenges of the NIA to enhance the system's trustworthiness, and security requirements, as well as address the privacy concerns that face such systems.

1.2 Protection of Electronic Identity Systems (EIS) through policies

Electronic Identity Systems (EIS) are platforms used to collect, process, store, manage, retrieve, and disseminate personal identification information for various purposes, including economic, social, and political. There are different types of these systems based on their characteristics. While some of them allow online verifications, others do not. Despite these differences, such systems are increasingly central to national infrastructure, enabling access to services in areas such as healthcare, finance, and governance. Examples include Estonia's Digital Identity System and India's Aadhaar, both of which demonstrate the transformative potential of EIS in enhancing administrative efficiency and citizen engagement (World Economic Forum, 2018, Madianou, 2019).

In this thesis, EIS are examined not just as technical systems, but as socio-technical infrastructures that require robust governance and public trust. This makes the role of policies, particularly those related to information security and privacy, critical.

Information Security Policies (ISPs) are formalised rules and procedures designed to protect information systems and data from unauthorised access, use, disclosure, disruption, modification, or destruction (UK Government, 2025). These policies are essential for maintaining the confidentiality, integrity, and availability of data—principles often referred to as the CIA triad (Whitman & Mattord, 2018).

Privacy policies, in contrast, govern the ethical and legal handling of personal data—how it is collected, used, shared, and retained. While both ISPs and privacy policies aim to protect data, ISPs are typically broader and more internally focused, addressing technical and procedural safeguards. Privacy policies, on the other hand, are externally oriented, focusing on data subject rights and compliance with legal standards (Solove, 2006).

Importantly, privacy and security are deeply interconnected. One cannot ensure privacy without adequate security controls. This is reflected in legal frameworks such as the UK Data Protection Act 2018, which implements the General Data Protection Regulation (GDPR) and mandates appropriate technical and organisational measures to secure personal data (ICO, 2023).

EIS are typically operated by public sector organisations, which are subject to additional legal and ethical obligations. These include not only data protection laws but also sector-specific regulations such as the Freedom of Information Act 2000, which imposes transparency requirements. Public sector data governance is therefore shaped by the need for public accountability, legal compliance, and citizen trust (Bannister & Connolly, 2011). A useful way to understand these differences is by comparing how privacy policies operate in the private versus the public sector as detailed in the table below:

Aspect	**Private Sector**	**Public Sector**
Goal	Customer trust, legal	Public accountability, legal mandate
Legal Basis	GDPR, Data Protection Act 2018, CCPA, PIPEDA	Data Protection Act 2018, Freedom of Information Act 2000, Public Task, Legal Obligation

Oversight	Internal Compliance teams, Information Commissioner Office (ICO)	Regulatory bodies (e.g. Information Commissioner Office (ICO)
Transparency	Market Driven	Legal Requirements
Trust Mechanism	Brand reputation	Public Interest and Scrutiny

Table 1:Comparism of Privacy Policies in Public and Private Sectors

This thesis focuses on the public sector, specifically the Ghanaian National Identity System. It examines how information security and privacy policies are formulated, implemented, and influenced by internal and external factors. In doing so, it contributes to a deeper understanding of how EIS can be protected and trusted in a public governance context, where transparency, accountability, and legal compliance are paramount.

1.3 Research Problems and Questions

Electronic identity systems are expected to play a central role in national infrastructure, handling sensitive personal information and supporting both government and private sector services. These systems must gain public trust by ensuring robust security measures. “Trust issues are the least concrete to deal with and there are multiple valid ways of looking at trust” (McCall et.al., 2012).

Despite the extensive literature on organisational information security, there is a lack of research on managing the security of electronic identity systems specifically. This study aims to fill this gap by exploring the interplay between human factors, processes, and governance in the context of EIS. Additionally, the research aims to investigate the development, implementation and evolution processes that such systems’ ISPs could consider to ensure effective and efficient organisational data and system security.

To do this, we posed the following research questions:

> **RQ1:** What do the information security requirements of identity systems mean to the NIA information security policies?
>
> **RQ2:** Should NIA ISP be expressed, formulated and implemented differently?
>
> **RQ3:** What internal and external factors affect the NIA ISP expression, formulation and implementation?

1.4 Methodological Approach

This research employs a mixed methods approach to investigate the awareness, understanding, and involvement of stakeholders in the NIA's information security policies. The NIA was chosen as a case study due to its significant role in Ghana's national identity management and its interactions with various government and private sector organisations. The methods used include literature surveys, questionnaires, and interviews with both internal and external stakeholders. Specifically, the researcher adopted an Instrumental Case Study design to find answers to the above research questions through the following tasks:

1. Background literature review on Electronic Identity Systems: We researched to understand identity systems and their forms or types and what such systems do. We assessed the Identity systems in Estonia (Estonian Digital Identity System) and India (Indian Digitised Identity System) by reviewing current works done on them to understand the systems' features, the cards, status and security controls to protect those systems. With the supervisor's permission, we also tried to get some pointers/clarifications from some individuals with experience with the Indian System. We sought their views on their experiences with the systems and their opinions on its security.
2. Background review on Information Security: We researched Information Security Management to have a general overview of policy formulation and implementation processes such as Security planning, Security Analysis, Security Design, Security Implementation, Security Review and Continual Security. We also researched how to analyse Information Security Policy documents to know their effectiveness. From the readings, we identified metrics used to assess ISP documents, such as the use of breath, clarity, brevity, content, and readability, among others.
3. Case Study Research Methods: Having established the research questions based on readings, we researched the research methods and identified the suitable ones that could best answer the research questions.

Based on the internal and external organisational structure of the NIA, we designed the following:

- NIA Staff Survey: The NIA Junior and Middle staff questionnaires were with closed questions using Likert scales, and it was conducted on paper. The participants were 115 and three were discarded after quality checks. The study aimed to understand the perception and beliefs of the junior and middle staff and their extent of involvement in the development, enforcement, evolution and compliance with the NIA ISP.

- NIA management Interview: The management interviews were semi-structured with both current and past management members. The participants were 9 in total and the study aimed to understand the senior management perspective about their perceptions and thoughts about Information Security (IS) effectiveness, IS management and ISP.
- NIA user agencies Interview: The NIA User agencies' interviews were semi-structured with current nominated management members. The participants were 13 in total and the study aimed to understand the external stakeholders' (user agencies) views and perceptions about their involvement in the NIA ISP development, implementation, and evolution.
- General public Survey: The General Public questionnaires were with closed questions using Likert scales, and was conducted on paper. The participants were 155 and seventeen were discarded after quality checks. The study aimed to understand the public's perception and beliefs about the formation, expression, and evolution and trust issues.

The reason for adopting this mixed methods approach is to provide a comprehensive understanding of the theoretical problems relating to ISP compliance, formation, implementation, and evolution within the Ghanaian Identity System environment. Each study aimed to gather detailed insights from different stakeholder groups to ensure a holistic view of the issues at hand.

1.5 Research Outcome

The main findings of this research reveal several key insights into the awareness, understanding, and involvement of stakeholders in the NIA's information security policies.

Firstly, while there is a general awareness of information security policies among NIA staff, significant gaps exist in their understanding and involvement in policy formulation and implementation. Many staff members are aware of the policies but lack a deep understanding of their content and the rationale behind them. This gap suggests a need for more comprehensive training and communication strategies to ensure that all staff members are not only aware of but also understand and can effectively implement these policies.

Secondly, the research highlights varying levels of trust and engagement with the NIA’s security measures among external stakeholders, including user agencies and the public. Some external stakeholders express confidence in the NIA’s security protocols, while others are sceptical and less engaged. This variation underscores the importance of building stronger relationships and trust with external stakeholders through transparent and inclusive policy development processes.

Additionally, the study finds that all stakeholders, both internal and external, believe they should be involved in the development and evolution of the ISP of identity organisations. This involvement is seen as crucial for ensuring that the policies are comprehensive, practical, and widely accepted. The research also indicates that stakeholders have high expectations for information security management from identity organisations, emphasising the need for robust and effective security measures.

Furthermore, the findings suggest that while the fundamental principles of information security are similar across different sectors, there is an increased emphasis on information security within identity organisations due to the significant impact of potential security breaches. This highlights the additional challenges faced by public sector organisations in managing information security.

Overall, the research outcomes emphasise the necessity for both internal and external stakeholders in businesses, organisations, and governments to understand and comply with their ISPs. It underscores the importance of employee awareness and compliance in securing personal data and preventing organisational vulnerabilities. These findings contribute to improving responsible behaviour among employees and other users, thereby enhancing the overall security posture of EIS organisations.

1.6 Research Contributions

This research makes several significant contributions to the field of information security, particularly in the context of electronic identity systems (EIS).

Firstly, it provides detailed insights into the specific challenges and requirements of managing security within EIS. By examining the perspectives of both internal and external stakeholders, the research highlights the complexities involved in ensuring robust security measures in identity management systems. This includes understanding the unique security needs and expectations of different stakeholder groups.

Secondly, the study underscores the critical importance of stakeholder involvement in the development and evolution of information security policies. It demonstrates that inclusive policy development processes, which actively engage both internal and external stakeholders, can lead to more effective and widely accepted security policies. This finding is particularly relevant for identity organisations that must balance the needs and concerns of a diverse range of stakeholders.

Additionally, the research offers practical recommendations for improving the effectiveness of information security policies in EIS. These recommendations are based on the empirical data collected through mixed methods, including literature, surveys, and interviews. The study suggests that comprehensive training programmes, transparent communication strategies, and regular policy reviews are essential for enhancing stakeholder understanding and compliance with security policies.

Furthermore, the research contributes to the broader field of information security by confirming the importance of combining human and technological approaches to protect organisational data and systems. It also highlights the impact of motivation on ISP compliance and enforcement, providing valuable insights for policymakers and practitioners aiming to improve security practices within their organisations.

It also outlines key issues that affect government-controlled EIS systems and suggests how those challenges such as political appointments; government interference, public-private partnerships, and public sector staff management constraints could be addressed to ensure effective information security management.

Overall, this thesis advances our understanding of the critical factors that influence the development, implementation, and evolution of information security policies in electronic identity systems. It emphasises the need for a holistic approach that considers the perspectives of all stakeholders and provides actionable recommendations for enhancing the security and effectiveness of these systems.

1.7 Dissertation Outline

This dissertation is organised into eight chapters:

Chapter 2 presents the Literature Review by providing an overview of existing research on electronic identity systems, information security policies, and information security management.

Chapter 3 presents the Research Methodology by detailing the research design, including the case study selection of the NIA and the mixed methods approach.

Chapter 4 presents the survey study of the NIA staff.

Chapter 5 presents the interview study of NIA's current and past management.

Chapter 6 presents the interview study of NIA user agencies.

Chapter 7 presents the survey study of the general public about the NIA.

Chapter 8 presents the main conclusions of the thesis, its contributions and recommendations for practices, research and further work.

2 Background and Related Work

This chapter discusses the background and related works in the existing reviewed literature about Electronic Identity Systems (EIS). It further highlights the context of this research and assesses the security requirements and effectiveness of Information Security Policies (ISPs) in EIS. The chapter also provides insights into the types and examples of such EIS systems, their benefits, and critical concerns such as EIS trustworthiness and privacy. Such concerns or problems are necessary and worth researching within the context of Information Security Policies in Identity Management to ensure enhancement in ISP compliance, development, implementation, and evolution through identifying threats, vulnerabilities, awareness, and comprehension of the organisation's security policy.

The chapter is organised as follows: Section 2.1 outlines Electronic Identity Systems, their advantages, and the characteristics of a good EIS. Section 2.2 focuses on the types and examples of EIS systems and the need for providing security for such EIS and the data and discussion on digital and digitized identity systems. Section 2.3 explains security concerns about EIS and the necessary controls to manage such systems to address the concerns that people have about such systems. Section 2.4 discusses the security concerns in EIS and the controls used to address such concerns. Section 2.5 discusses what Information Security (IS) is. Section 2.6 focuses on why information security is essential. Section 2.7 discusses the role of information security policies in information security assurance, IS effectiveness, IS management, and information security policies. Section 2.8 presents the research gap identified from the literature. Section 2.9 presents the conclusion of this chapter.

2.1 Electronic Identity Systems

Electronic Identity systems (EIS) are used to collect, process, store, manage, retrieve, and disseminate personal identification information for economic, social, and political purposes. The systems are used to process identity data about individuals to create value for organisations, businesses, and individuals through verification of the identities (World Economic Forum, 2018). An identity is "a collection of characteristics by which a person is defined, recognised, or known" (Just & Renaud, 2012) and "it includes information such as their name, their date-of-birth, as well as other information about themselves, their preferences and behaviours, etc" (Just & Renaud, 2012).

According to the United Nations Report on Identity (2018), over one billion people worldwide cannot prove their identity. In the case of Africa, “about 542 million people in Africa do not have a foundational identification and therefore are “invisible” (African Union, 2020). The report indicates that out of this number, around 95 million children under five have never had their births recorded, and 120 million children do not have a birth certificate. This justifies the need for the development and management of such systems to provide a form of identity to such persons.

To address these challenges, governments and organisations are turning to digital technologies to modernise identity systems. The digitisation of identity aims to bridge the gap between the identified and the unidentified, enabling broader inclusion and more efficient service delivery. EIS play a pivotal role in this transformation by offering scalable and secure solutions for identity verification.

2.1.1 Advantages of Electronic Identity Systems

The digitisation of identity systems has recently had economic, social, and political impacts on countries that have implemented them (Anthopoulos et al., 2007). To this effect, several governments and private sector businesses have acknowledged the critical role that Identity Systems play in developing and sustaining their economies. For instance, Anthopoulos et al., (2007) note that governments have taken the move to provide a one-stop point of access for their citizens to access services by using Digital Identity Systems to achieve socioeconomic and political development.

On the economic front, countries like India and Ghana use Identity Systems to enhance service delivery to their citizens. This has primarily facilitated access to benefits, rights, and services. It has also helped improve public administration, planning, and service delivery by reducing fraud and revenue losses (UIDAI, 2018). For instance, in India, banks, the telecoms industry and other companies have effectively carried out their functions without much hindrance due to the development of the Aadhaar Identification system (Ghosh, 2016). The telecoms sector uses the 12-digit Aadhaar number to verify the individual's identity and issue the person with a Subscriber Identity Module (SIM) card in 5 minutes (S. Ghosh, 2016). In the case of Ghana, the country uses the 13-digit National ID PIN for identification purposes to provide financial services like account opening or mobile phone SIM card purchase (Duodu, 2018).

The Digital Identity System also helps provide social support to people. The system enables governments to know the total population in a geographic location and the types of social services like schools and subsidised housing that must be provided to the residents. In India, for instance, the Aadhaar System has effectively helped the government verify citizens' identity to provide services. The Indian government also pays subsidies to the less privileged in the identified areas by simply authenticating the Aadhar number of the beneficiary and proceeding to pay in record time (Ghosh, 2016). This payment has positively impacted the social needs of the vulnerable in India.

On the political front, Identity Systems are used by governments to conduct elections. For instance, the government of Estonia uses digital identity in a system called “i-voting” for online voting activities (Information System Authority, 2019). Estonia is the first country in the world to hold nationwide elections using the internet voting system. It also became the first country to conduct parliamentary elections in this same manner. The online voting in the case of the Estonian Identity System highlights the extent to which a Digital Identity System has been used. In the case of India, it is the most extensive digitised identity system currently being built in the world and they use Electronic Voting machines (EVMs) to verify the identity of their voters through electronic means before they are allowed to vote manually.

2.1.2 Good Electronic Identity Systems

According to the World Economic Forum report on Identity (2018), good digital identities and Digitised Identity Systems must have five essential elements. The elements are:

- Fit for purpose: The system is reliable for individuals to build trust when exercising their rights and freedoms and accessing services.
- Inclusive: This is where anyone wishing to use the system is freely allowed to do so without any identity-related or authentication discrimination.
- Useful: Good identity systems must be easy to establish and use and provide access to valuable services.
- Offers choice: Good systems enable individuals to consent to how their identities would be used.
- Secure: Good systems should protect individuals, organisations, devices, and infrastructure from “identity theft, unauthorised data sharing and human rights violations” (World Economic Forum, 2018).

2.2 Types and Examples of Systems

This section focuses on the types and examples of EIS systems and the need for providing security for such EIS and the data.

2.2.1 Digital and Digitised Identity Systems

Organisations and governments have used different terms to describe the identity systems that they set up based on their scopes and functionality. These Identity systems fall under two main broad classifications to meet the needs of these organisations, governments, and businesses. The identity systems are used to carry out either online identification or to identify an individual electronically. Depending on the country's focus, businesses or organisations often use terms such as digital identity systems, digitised identity systems, and identification systems.

Digital Identity Systems are both more extensive in scope and functionality. Digital Identity Systems go beyond the collection and storage of personal data. The significance of digital identity systems in managing populations, improving public service delivery, and enhancing national security is crucial (Atick, 2016). Digital Identity Systems cover how other services are available to other stakeholders electronically. The Estonian System is an example of a digital Identity System. That system is considered part of an Electronic Government System with a broader mandate to develop and manage secure data exchanges (X-Road, document exchange). The data exchanges are done between institutions, providing an overview of state information systems and data (RIHA), the use of electronic identity, supervising the functioning and protection of the state broadband network, organising e-elections, protecting, and supervising the activities of the State Portal and the work of the ID card help centre (Information Systems Authority, 2024),

Digitised Identity Systems, as in the case of India (Ghosh, 2016), Malaysia (Loo et al., 2009), and Ghana, are where countries build systems by collecting and storing personal data for basic identification-related services. These digitised identification systems have changed the social, political, and economic lives of people (Corrocher & Ordanini, 2002; Gukurume & Mahiya, 2020). Digitised Identity Systems are generally not digital and are standalone systems. This means their scope and functionality are limited compared to Digital Identity Systems. An example of such a limitation is the absence of online identification.

Interestingly, most governments and organisations are building and using such digitised systems as an intermediate step to develop digital ones for the future where both physical and online identification can be carried out to provide enhanced services, choice, trust, and rights to the citizens and residents. This is because establishing these systems ensures that choice, trust, and rights are available to the individuals whose personal data has been collected (World Economic Forum, 2018).

To better appreciate the similarities and differences between Digital and Digitised Identity Systems, we focused more closely on comparing the Indian and Estonian systems. The choice of these systems is based on the fact that the Indian system is the biggest in the world to be developed, which has generated so much attention. In contrast, the Estonian system is generally believed to be the most sophisticated system in the world.

2.2.2 Indian Identity System

The Indian Aadhaar Identity system is an identification system where individuals enrol and are assigned an Aadhaar number with a 12-digit unique number. They developed the system based on “developed policies, procedure and system for issuing Aadhaar numbers” (UIDAI, 2018).

“Aadhaar” is a Hindi name which means “foundation” or “Base”. The Government of India adopted the word to refer to the identification system in India and, by extension, the Act establishing the system. The individual gets the Aadhaar number for identification. The Aadhaar number is required to ensure the security of an individual's identity information and authentication records.

During registration, they capture the personal biometric data, including the ten fingerprints, signature and the individual's iris. In the case of children, they are eligible to obtain numbers from birth, but their numbers are linked to the parent’s biometrics until they are old enough to provide their own after five years of age (Greenleaf, 2010). Third-party registration officers, referred to as “registrars” for each state, do the registration process. According to the UIDAI, a registrar is an entity authorised or recognised by UIDAI for enrolling individuals. The registrar also appoints enrolment agencies responsible for collecting individuals' demographic and biometric information during enrolment. They forward the collected personal data to UIDAI for recording in the Central Identity Repository (CIDR). The CIDR is a centralised database that stores all Aadhaar numbers and the citizen and residents’ corresponding demographic and biometrics (UIDAI, 2018). When the UIDAI authenticates the records, they send a letter to the agent and the applicant with the Aadhaar number provided.

The letter has a detachable portion that contains the Aadhaar number for the applicant to laminate and keep.

The card issued is non-smart, with the individual's portrait laminated with a barcode imprinted. The reason is that the identification authority believes the Aadhaar number is enough to verify and authenticate identity once provided (UIDAI, 2017). The card contains personal information about the individual, such as name, Date of birth, gender, photograph, residential address and the 12-digit PIN.

According to UIDAI, one can update their biometric information only under the following:

- When a child turns five years
- When an individual is involved in an accident or other incident that has altered his physical features.
- Ten years after registration.

It is essential to state that the UIDAI is solely for establishing the standards and procedure for enrolment. However, the Indian government and state (union) governments are the ones to recruit enrolment officers and provide the needed resources for registration to ensure that the state departments perform their roles; they sign a Memorandum of Understanding (MOU) with UIDAI.

2.2.3 Estonian Identity System

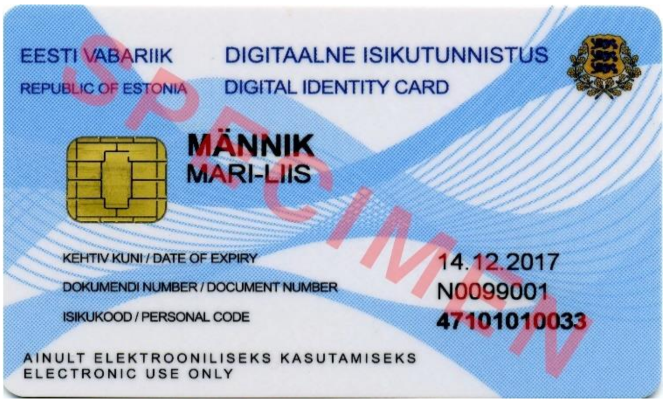
The Estonian system is considered the most effective and efficient digital electronic governance system, which has made other countries focus on developing such a system (Kalvet, 2012). The system shows how personal identity data is a basis for enforcing individuals' rights and providing access to essential services such as health, education, financial, social protection, and mobile connectivity through an electronic Government System. According to the ISA (2019), a standard application for an ID card is made within 30 days (of the acceptance of the application and commencement of proceedings) when the submission is made in the client service office or a foreign mission of the Republic of Estonia. However, delivering an ID card to a foreign mission may take more than 30 days.

An ID card can be applied for in an expedited order, and this request is handled within five working days only in the service offices located in Tallinn, the capital of Estonia. However, one cannot apply for an expedited service if it is their first time applying for an ID card (Information System Authority, 2018). One condition for registration is the applicant's physical presence and verification by issuance authorities at a service point during the first issuance (Information System Authority, 2019).

Alternatively, a Digi-ID can be applied in addition to the Identity Card at the service points of Police and Border Guards that are used for electronic purposes only. Digi-ID is “a digital identity card that can be used for personal identification and digital signing in the electronic environment” (Information System Authority, 2019). According to the Information System Authority (2019), the Digi ID is an application that enables citizens and residents to electronically sign documents online through either their mobile phones (Mobile ID) or through a downloaded app (Smart ID). According to the Information System Authority (2019), the Digi-ID provides the “easiest, fastest and safest way to authenticate yourself online”.

It is essential to state that changes to biometric information, spelling corrections and contact details are done by the service points of the Police and Border Guard Board or the foreign mission before the data is sent for processing and card issuance (Police and Border Guard Board Certificate Policy, 2022).

After the first issuance of the card, they do subsequent renewals without physically being present for verification at a Police and Border Guard Board or the foreign missions office (Police and Border Guard Board Certificate Policy, 2018). A sample of that ID as below:



EESTI VABARIIK
REPUBLIC OF ESTONIA

DIGITAALNE ISIKUTUNNISTUS
DIGITAL IDENTITY CARD

SPECIMEN

MÄNNIK
MARI-LIIS

KEHTIV KUNI / DATE OF EXPIRY 14.12.2017
DOKUMENDI NUMBER / DOCUMENT NUMBER N0099001
ISIKUKOOD / PERSONAL CODE 47101010033

AINULT ELEKTROONILISEKS KASUTAMISEKS
ELECTRONIC USE ONLY

Figure 1: Sample of Estonian ID Card

The term “Card” is used to collectively refer to several different types of cards for the following different groups of people captured in the Police and Border Guard Board Certificate Policy (2022):

- Identity card for Estonian citizens
- Identity card for European Union Citizens

- Digital Identity Card for Estonian Residents
- Digital identity card for e-residents
- Residence permit for long-term residents
- Residence permit for temporary residence citizens
- Residence permit card for family members of citizens of the European Union
- Diplomatic identity card.

The card, in general, has the following features:

- The card captures primary personal data such as first name, surname, Date of birth, Public PIN, Gender, Date of Issue, Signature of the individual, portrait, and expiry date on a plastic smart card with a chip embedded in it in addition to a barcode.
- The card also contains an unchangeable 11-digit Personal Identification number, machine-readable code, changeable laser image in the form of a personal identification code which changes colour when tilted, and micro text with lines.
- The system also gives individuals two PINs. A Public PIN and a Private PIN. The use of the Private PIN is considered to be equal to physically signing a document.

Estonian citizens can use their ID cards to travel in European Union member states and European Economic Area countries. However, a different ID card is issued to the citizens of the European Union. An EU citizen ID card is not valid as a travel document. The Estonian ID card is valid for up to five years.

From the two systems, the research highlights that a unified national strategy focused on the type of EIS, robust enrolment processes, and strong data protection measures are essential for the success of e-ID systems. Additionally, effective governance, privacy-by-design, and interoperability are essential components for the success and sustainability of Identity systems. Achieving these requires the need to manage the security concerns related to such EIS identity systems.

2.3 Security Concerns in Electronic Identity Systems

Organisations, businesses, and governments continuously acknowledge the immense benefits of information to their survival. All organisations “are supposed to protect the information they store due to its effect on the organisation’s sustenance and growth” (Raggad, 2010). Many organisations recognised the benefits of information security long ago (Culot et. al., 2021; Cram et. al., 2017). In recognition of this importance, organisations place employees in cabinets to protect their paper records (Alkhurayyif & Weir, 2017). Due to this, organisations and businesses have changed their operational strategies and environments from closed environments with mainframe computers to complex environments by working on distributed networks, including the Internet (Safa et al., 2016). This, in effect, has "changed the information assets of organisations into electronic forms, which are processed by information systems and communicated through the Internet" (Alkhurayyif &Weir, 2017). In effect, what this means is that information security is required, especially when the technology applicable to information has risks (Blakley et al., 2002).

Electronic Identity Systems are forms of information systems and therefore require adequate security protection. To this effect, most organisations, governments and businesses that deal with information systems and electronic identity systems continuously rely on technology and online data storage to provide more competitive services and support to their citizens and customers. Taylor et.al (2020) assert, "Any business will have information that is critical to its continued effective operation". Knapp et al. (2009) also acknowledge the reliance of organisations on Information Systems for their operations despite the growing security threats that relate to such systems, whether digital or digitised. According to Baskerville (1993), "The security of information systems is a serious issue because computer abuse is increasing. For instance, OnePlus, a Chinese phone company, in 2018 alone, lost more than 40,000 online customers' credit card details (Orlowski, 2018). British Airways system was also compromised due to exposure, and as a result, over 380,000 personal and financial details of customers were compromised (Claburn, 2018b; Spero, 2018). According to Leyden (2017), 1.4 billion data records were exposed in 2016, and data compromise was 86 per cent over the previous year. In 2015, 90 per cent of large companies experienced security breaches in the United Kingdom alone, while almost three-quarters of the small companies also reported breaches (PwC, 2015). According to Verizon report, 74% of all the recorded breaches had a human involvement either through error, privilege misuse, use of stolen credentials or social engineering (Verizon, 2023). This is the reality in the operations of companies and government service organisations. Kunz et al. (2011) sum up these negative effects of information security by concluding, "With this intensified exchange, information security becomes a major issue".

Many people have also expressed several reservations about Identity Systems due to the adverse effects they can cause. For instance, Lyon and Bennett (2008) note that "Once cards are mandatory, then they may be used to single out or even to harass visible minorities and those with alternative lifestyles" (Lyon & Bennett, 2008). Fussell (2001) also notes, "The inclusion of ethnic identity on ID cards in Rwanda in the 1990s was an instrument of genocide". He further explained that there is the potential for abuse against marginalised groups and how group classifications on ID cards also "played important roles in facilitating the large-scale expulsions of tens of thousands of persons on account of their group identity from Bhutan in 1991 and Ethiopia in 1998" (Fussell, 2001).

Some also have reservations about the need to ensure equal citizen access to supporting infrastructure (Ohemeng & Ofosu-Darkwah, 2014). This is due to how emerging Identity Systems collect sensitive information about individuals as they could be used for other negative acts.

Despite the above, other key concerns by individuals focus on privacy, trustworthiness, Authentication and Authenticity of the system. Privacy is a fundamental human right (Equality and Human Rights Commission, 2021). Privacy is "the claim to or the right of individuals to exercise a measure of control over the collection, use and disclosure of their personal information" (Kwame Adjei, 2013). Users will likely avoid using an Identity System if they perceive that their personal information will be subjected to various privacy abuses (Kwame Adjei, 2013). Addressing privacy concerns and demonstrating value compatibility can improve the acceptance of citizen identification systems (Cofta, 2008).

Regarding Trustworthiness, it is the reliability or decision support of a person, system, or something in a given situation (Gambetta, 1988; McKnight & Chervany, 1996). Trustworthiness describes the extent to which a system can be relied on to achieve its intended purpose. In the specific case of Identity Systems, the issue of trustworthiness can be used to refer to the reliability of the systems in identifying people correctly and ensuring the protection of the privacy of the personal data collected. Cahill et al. (2003) indicate that "Humans use trust daily to promote interaction and accept risk in situations where they have only partial information". Trust is also seen as a critical foundation of an effective identity and is shaped by confidence in the systems that create and manage user identities (Grant, 2011). According to Kubicek and Noack (2010), a "better understanding of the perceptions of citizens should open the way for better design and implementation". To Jones and Moncur (2020), Trust is defined in many ways across disciplines, but the persistent theme is risk and uncertainty in a decision. To this effect, the trustworthiness of an ID system needs to be geared towards how efficiently it can be relied on to achieve its intended purpose. Similarly, trust in government, its agencies and other organisations by citizens have received increased attention in recent times (Panel on Civic Trust and Citizen Responsibility, 1999; Sims, 2001). Even more important is the conclusion by researchers that focused on Western Europe that trust in government is indispensable for government to function (Bouckaert & Van de Walle, 2003).

Regarding Authentication, it is the process of verifying the identity of an agent, human or system before granting access using a user ID and a password or a smart card, public critical infrastructure or biometrics (Raggad, 2010).

Authenticity is the process of ensuring that the origin of transmission of personal data is correct and that its authorship is also valid (Raggad, 2010).

The above therefore highlights the calls for providing adequate security to protect and secure the people, the hardware, the software, the network, and the intruders. This ensures the confidentiality, integrity and availability of the system and data for social, economic, and other benefits. Despite this, Karlsson et. al., (2016) acknowledge that there is a predominant focus on management and technical issues about information security issues with less focus on the human factors.

This means that Identity systems have to be effectively managed to reduce these critical concerns raised regarding the protection and security of data against attacks. This can be done by providing the necessary technical, operational, and managerial controls (Raggad, 2010) as well as the human factor issues.

2.3.1 Technical Controls

They are the security measures that the computer system executes, and they can essentially provide automated protection from unauthorised access or misuse, facilitate the detection of security violations, and support security requirements for applications and data. To Taylor et al., (2020), “technical controls are implemented to provide protection against security incidents”. These technical controls use software and data to detect network intrusion, encryption, and access control (Raggad, 2010). Both technology and network security fall within technical controls that organisations put in place to ensure data confidentiality, integrity, and availability. Technology security is adopted to protect and support software and hardware that perform enterprise operations. It usually deals with attacks that come through intrusions. Such mechanisms are done to prevent dangerous consequences.

Network security protects the interconnection of computers and other services from unauthorised access or modification, disclosure, or destruction of the users' data (Raggad, 2010). All host-based security is reviewed periodically, and equipment such as laptops, routers, switches, bridges, hubs, etc., are well protected and reviewed against malicious attacks.

As part of the technical control measures, the Estonia System, for instance, uses cryptographic keys to provide the necessary security to the user. This is due to the investment made to protect the identity management system.

2.3.2 Operational Controls

They primarily address security mechanisms operated by people and they require technical or specialised expertise by relying on management activities. Operational controls include personnel security, physical and environmental protection, contingency planning, incidence security, media protection and maintenance. The security measures cover procedures, regulations, policies, standards, and protocols of interactions within the information system environment (Raggad, 2010). In Estonia and India, for instance, the registration procedures are clearly outlined to ensure ease of access and compliance with organisational policies by user agencies and citizens.

2.3.3 Managerial Controls

They focus on the management of the information system and the management of risk. They include techniques such as risk assessment, planning, certification, accreditation, security assessments, and system and service acquisition that require management's actions.

In an effective Information Security Management, personnel, procedural, Information Technology and Network Security issues are considered and used to form the basis for operational, managerial, and technical control measures for the business or company to achieve its objectives. Large and small organisations have now recognised the need to engage in robust information security management to protect the computing environment by providing personnel security, procedural security, data resource security, software and hardware security and network security (Raggad, 2010). Personnel security involves the work of people, processes, and activities in the organisation. This means that employees can be a security threat, intentionally or unintentionally, hence the need to undertake personnel security. Personnel security is about practices and tools adopted by the human resources unit to ensure the security of their staff through security training and non-disclosure agreements, among others (Raggad, 2010). Taylor et al., (2020) explain that organisations have to train both their employees and third parties accessing their information to comply with their policies and procedures to reduce assurance issues.

The technical, Operational and managerial controls are generally expected to conform to national and International Security Standards. The International Security Standards that are acknowledged include the National Institute of Standards and Technology (NIST) and the International Organisation for Standardisation (ISO). These systems are forms of Information Security Management Systems that aim to provide solutions to organisations, businesses and institutions. For instance, the ISO is built based on "a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security" (Taylor, 2013; Taylor et al., 2020). According to Taylor et al. (2013), "it is considered good practice to base an effective information assurance management system on the principles of the relevant standard" and, "the use of an internationally accepted standard such as the ISO/IEC 27000 series makes sense in the global nature of operations today". The ISO provides guidance, standards and information required to ensure effective IS and IS management. The details relate to managing Threats, vulnerability, risk and impact of such systems, employees and data handling. The ISO recommends the need to ensure IS, ISM and guidance on ISP development, management and implementation. More specifically, it encourages Information security to be part of company policy, standards, guidelines and procedures documentation.

The ISO also deals with other key issues such as the importance of information security as part of a business model and its impact on security, Corporate governance and related areas of risk management and the role of information security in countering hi-tech and other crime among others (Taylor et. al., 2013).

2.4 Why the Focus on Security Concerns in Electronic Identity Systems

Recently, the management of information systems and their security have received considerable attention. As noted by Karlsson et al. (2017), "Information and information systems have become critical assets in most organisations". Farooq et.al. (2015) argues that

“Effective information security (IS) programmes should be designed keeping in view the objectives and mission of the organisation”. Against this background, investments, and maintenance in systems, technology, and online data storage have been the focus of most technology-reliant organisations, governments, and businesses. Even more critical is when such systems are used to collect, store, or manage individuals' data due to the data's sensitivity and some security concerns that people have about such electronic identity systems. This has called for the need to use security controls to protect the valuable information that organisations must use to achieve their business objectives nationally and internationally. It is even more important for EIS organisations due to the potential threats of identity theft, privacy concerns and trust issues from the stakeholders and members of the public. For instance, to prevent such occurrences, the UIDAI and the Estonian System do not collect information on a person’s race, religion, caste, tribe, ethnicity, language, income, or health (Greenleaf, 2010). The reason for this is due to previous “episodes of communal, ethnic, and religious violence” (Greenleaf, 2010). However, it is only under exceptional circumstances that the UIDAI is mandated to collect demographic information such as those outlined above. Lusoli and Miltgen (2009) highlight that “there are high perceptions of risks, both general and contextual” and that “most young people are sceptical of the internet as an environment for the exchange of personal data and have major doubts about personal data protection”. Lusoli and Miltgen (2009) also noted that young people “perceive high risks in giving personal data and fear that these will be misused in specific eService settings”. Additionally, “Just over a quarter of social network users (26%) and even fewer online shoppers (18%) feel in complete control” (Eurobarometer 359, 2011) as far as their data is concerned.

According to Greenleaf (2010), governments and organisations need to be able to protect vulnerable groups such as women, children, senior citizens, persons with disability, migrant unskilled and unorganised workers, nomadic tribes, or those without permanent residential locations, among others when using such systems.

Again, users must be given privacy assurances during and even after the personal data collection. This is because the assurance and protection of privacy can lead to effective “secure and trusted systems” (Kwame Adjei, 2013). For instance, India’s UIDAI has put specific measures in place to ensure individuals' and data privacy by providing a general prohibition against staff or the authority from revealing information stored in the CIDR except during authentications permitted by law, such as for national security purposes (Greenleaf, 2010) or as instructed by a competent court. Again, the Indian Digitised System has adopted randomisation of the Aadhaar number to protect the privacy of the individual as it does not reveal the person's personal information simply by using or disclosing the number (Greenleaf, 2010). Additionally, Greenleaf (2010) highlighted that the individual's privacy is further protected because the UID cannot be used to restrict the movement of a person or access to work compared to other areas where the ID cards are used as passports. This is because people cannot be discriminated against based on the information displayed on their ID cards. In India, the Aadhaar number, by Law, cannot be used to restrict the movement of a person or an individual but can only be used to identify an individual. The individual is also given the right to access his personal information when he requests it and can also request changes to their demographic information. However, the biometric information cannot be changed through the request by the user except when the UIDAI has satisfied itself with the need for such change (Greenleaf, 2010).

Regarding trustworthiness and its concern by citizens, it requires that the sensitive data of this nature that are collected, stored and managed by EIS must be adequately protected to prevent tampering and unauthorised access and its potentially catastrophic impact on businesses, government, and individuals (Raggad, 2010). Information security to such systems is therefore highly important.

2.5 What is Information Security

Information security remains critical in today's organisations due to continued data breaches, system outages, and malicious software (PwC, 2016; Verizon, 2016). This is partly why an assessment of current IS literature highlights the continuous use of the CIA triad, which consists of Confidentiality, Integrity, and Availability (CIA) (Denning, 1999; Stoneburner, et. al, 2002; Gollmann, 2010; Waly, et. al, 2012). The three elements are used to ensure the protection and preservation of information. Confidentiality ensures that only authorised parties can access the information (Peltier, 2005; Andress, 2014; Taylor et. al., 2020). Integrity deals with the protection of information from unauthorised modification or deletion to ensure its data maintenance, its accuracy, and the modification by unauthorised users. Maintaining the integrity of data or information is crucial, so Organisations, businesses, and governments acknowledge the need for Information security to protect their interests by using multi-faceted strategies. These are required to prevent illegal access and reverse authorised changes as required (Whitman & Mattord, 2011; Andress, 2014; Taylor et. al., 2020). Availability is about users accessing requested information when needed. It guarantees that the organisational information is readily accessible to authorised parties only in a timely and reliable manner, without affecting productivity (Whitman & Mattord, 2011; Andress, 2014; Taylor et. al., 2020).

However, Dhillon and Backhouse (2000a) indicated that the CIA triad could not provide IS systems with the needed security. In addition to the confidentiality, integrity, and availability (CIA), they proposed the responsibility, integrity, trust, and ethicality (RITE) principles to "hold the key for successfully managing information security in the next millennium". Dhillon and Backhouse (2000a) believe that "responsibility, integrity, trust and ethicality (RITE) are considered important and are the first steps in securing the information assets of the organisation in the future". Dhillon and Backhouse (2000a) define the RITE as follows:

- Responsibility (and knowledge of roles): It is accountability for what went wrong in the past and handling future events and development in a particular sphere.
- Integrity (as a requirement of membership). It ensures that the employee recognises the data's value in his possession and that it is protected. Here, the employee is trained on the value of the data to the organisation and how to maintain the data using his values or integrity.
- Trust (as distinct from control). This is where an employee is expected to have more self-control and duty while his influence on supervision and external controls are reduced in his organisation.
- Ethicality (as opposed to rules). It ensures compliance with the "ethical content of informal norms and behaviour" (Dhillon & Backhouse, 2000a).

Donn Parker also proposed an additional three (3) components to information security in 2002. This, therefore, made the components six (6) in all. The six were made of the traditional three (3) that included:

- Confidentiality,
- Integrity,
- Availability

In addition, the new ones were:

- Possession

- Authenticity
- Utility

The six components make up what is referred to as the “Parkerian hexad.” It is essential to state that the Parkerian hexad considers the six components as atoms that could not be broken down into further elements, and all security breaches, irrespective of their nature, would be traced back to one or more of the six.

The literature further explains that Authenticity aims to ensure that the transmission origin is correct and that the authorship of the transmitted documents is valid.

In the case of Possession, it defines ownership or control of information. In contrast, Utility emphasises the usefulness of the information to decrypt it to make it meaningful to the intended recipient.

The National Security Agency (NSA) developed an information security training programme called the Information Assurance Training and Ratings Programme (IATRP). This programme did a triangular analysis of organisations' security postures and concluded in three sequential phases: Assessment, evaluation, and penetration testing.

The Assessment involves a high-level risk review of an organisation to effectively plan and recommend long-term directions for improving the organisation's information security needs. The Evaluation involves a detailed review of the strengths in enforcing an organisation's security policies and recommends medium-term directions on using technology to support the organisation's information security. It is mainly done internally with collaboration with all internal stakeholders. This action provides assurance, certification, and accreditation, informing the organisation of where the priority should be at a given time. The Penetration Testing is a technical activity identifies the vulnerabilities ready to be exploited by existing threats to the organisation. This action is invasive, non-collaborative, and involves external auditors and active penetration tests, among others.

According to Raggad (2010), attacks are organised in terms of three things: the identity carrying out the attack, the model employed in the attack and the effects of the attack on system owners. The effect of attacks on system owners is generally referred to as security disruptions. To this effect, Raggad (2010), explains that Information Security “depends on processes developed, documented and reviewed by owners to manage all interactions among the components”. Alkhurayyif & Weir (2017) states, “Security is a collection of features and services that deal with several security requirements by tackling a set of incidents”. Von Solms (2004) indicated that information security (IS) is largely multi-dimensional, and organisations must consider its importance to ensure the security or protection of their information assets and the environment. To him, an organisation's security “includes the physical security of buildings, fire protection, software and hardware, personnel policies and financial audit and control.”

Garber (2002) points out that different organisations have different security levels based on their security needs. According to Raggad (2010), the effectiveness of information security includes how the information is classified based on its value addition to the organisation and its sensitivity level and that, the value addition and sensitivity level define how much security must be provided to protect that information and classify whether it is public or confidential. If it is Confidential information, the information owners have to further define it under top secret, highly confidential, proprietary, or Internal usage information so that appropriate access and use can be granted as part of the security measures in the organisation.

Top secret information is internal data that is highly sensitive (highest sensitivity level possible) and considered the highest. When divulged, it can have a catastrophic impact on owners and the company (Raggad, 2010). Examples include strategic plans, acquisition information, military intelligence, etc.

Highly Confidential information is critical to the organisation’s operations and could hinder the capability of business continuity, but it is not a top secret (Raggad, 2010). The cost of replacing damaged items is primarily high and mainly relates to new technology, business plans, and products.

Proprietary information is also produced in-house and mainly relates to organisational resources like hardware, software, and methodology (Raggad, 2010). Examples are operational information and design specifications.

Internal Use Only information is confidential but not authorised to be made public, and the risk of financial losses is negligible when made public. Examples are minutes, announcements, and periodic reports.

This means that each organisation must consider the value of its data or information, the nature of the business or service they are providing, and the risks associated with such data to be able to employ the right strategy or approach in securing its business interests by reducing threats and vulnerabilities to the data or information. It is also essential to ensure the existence of a proper document in place that is clear, consistent, and available to the employees and all stakeholders. This can help in easy implementation and enforcement. The international IS standard, ISO/IEC27001, defines information security as 'protecting information from a wide range of threats to ensure business continuity, minimise business risk and maximise return on investments and business opportunities' (2001, p. 30). ISO 27001 "enable organisations of all sectors and sizes to manage the security of assets such as financial information, intellectual property, employee data and information entrusted by third parties" (ISO, 2024). This requires effective risk management.

According to the 2006 CISA Review-Journal, Risk Management is the process of identifying vulnerabilities and threats to information resources used by an organisation in achieving business objectives and deciding what countermeasures, if any, to take in reducing the risk to an acceptable level based on the value of the information resource to the organisation.

Risk Management starts with risk identification, then risk assessment and finally, risk mitigation. The risk management process is part of ensuring ISM in an organisation and is part of acceptable standards. These standards provide acceptable guidelines to manage risks and the impacts associated with threats, and vulnerabilities. Taylor et. al, (2020) acknowledge that understanding these risks and their impacts, threats and vulnerabilities is "critical to the whole of information assurance". Taylor et. al, (2020) explain that risk management consists of context establishment, risk assessment (risk identification, risk analysis, risk evaluation), risk treatment, communication and consultation, and ongoing monitoring and review.

Risk management adopts the use of controls as an IS framework to remove threats from occurring, reducing the impact of a threat, transferring the risk or accepting the risk by monitoring it (Taylor et. al., 2020). It also requires regular planning and assessment because the risks keep changing with time. This means that risk management and its maintenance are "a continual and iterative process that must not be allowed to whither through lack of action or a misplaced belief that the situation will not change" (Taylor et. al., 2020).

Providing an effective IS environment requires that the human aspect of Information security is considered to complement the technological applications (Safa et al., 2016). Lampson (2004), Sasse and Flechais (2005), and Schneier (2006) support the assertion that security is a "people" issue because humans are the ones in charge of implementing IS. Most information security breaches result from employees who violate policies (Herath, Rao, 2009; Nash & Greenwood, 2008; Siponen et al., 2014; Stanton et al.,2005).

Despite the above, some literature works point to some limitations to the CIA Triad. According to Raggad (2010), in the Star model, the CIA triad suffers from two drawbacks: its insufficiency in handling all security issues and its failure to include security management. Due to this, Authentication and Non-Repudiation have been added to make the triad a star.

Raggad (2010) explains that authentication is a mechanism designed to verify the identity of an agent, human or system before granting access. Usually, access is granted by requesting a user ID and password. The essence of this is to provide adequate security management. This provision can also be made using other methods like smart cards, biometrics, and public critical infrastructure.

Non-repudiation implies that neither end of the transmission process can deny their involvement in a transmission. This means the sender cannot deny sending the information, and the receiver cannot deny receiving that information (Raggad, 2010). Non-repudiation methods sometimes include using a digital signature, especially transmissions done via the Internet.

2.6 Why Information Security

It is widely accepted that all organisations depend on information for survival. It is, therefore, essential that timely, accurate and complete information is available to all stakeholders to be effective and efficient in their mandates. To ensure that accurate, timely, and complete information is available, there is a need to protect the data, activities, network, technology, and people in the computing environment adequately. To do this requires adequate information security, which addresses the security requirement issues (mostly threats and vulnerabilities) of the company or organisation and the overall objectives of the company through a “thorough study of the organisation’s business value generation model” (Raggad, 2010).

Additionally, Raggad (2010) advocates for the human or people-focused component as a key factor for ensuring security and explains that based on the four entity models. Raggad (2010) explains that the five (5) entities can root an attack on an activity, a person, a network, technology, and a data resource. He identified four models of attack, and they are outlined below:

- Probe model: The Probe Model is a passive attack designed to identify opportunities that can be explored to cause harm to the system owners. The attack usually takes any other conforming methods that the attacker explores.
- Infrastructure model: Infrastructure attack models are attacks that induce entities to cause harm to system owners by affecting the infrastructural attributes either fully or partially.
- Authorised access model: Authorised access models are attacks caused by insiders.
- Factory model forms of attacks are attacks induced by an entity to indirectly cause harm to system owners by modifying or substituting hardware or software at the factory or during the distribution process. They are primarily designed with remote access configurations to attack a computer system.

As Willison and Warkentin (2013) emphasise, although outside factors (e.g., external hackers and natural disasters) significantly threaten an organisation's information and technology resources, employees' actions are often viewed as a greater security risk. A fundamental approach to address the risks associated with such insiders is the adoption of Information Security Policies (hereafter, security policies), which specify the standards, boundaries, and responsibilities of users of information and technology resources to facilitate the prevention, detection, and response to security incidents (Bulgurcu et al., 2010; Lowry & Moody, 2015).

Knapp et al. (2009) acknowledge that policy enforcement is ongoing, and this helps management make it part of formal policies to keep workers in check. This is because, whether large or small organisations, there is a need to engage in robust information security by enforcing the rules and regulations that are designed by management.

2.7 The Role of Information Security Policies in Information Security Assurance

The term policy is interchanged with the term Strategy, while in other cases, the term denotes a specific response to repetitive situations (Ansoff, 1965). Policy has been defined in a planning and control context to establish limits of acceptable behaviour, decision confines, and standards (Davis & Olson, 1984). Policies are essential to information systems security as they provide the blueprints for an overall security programme and create a platform to implement secure practices in an organisation (Von Solms & Von Solms, 2004).

Higgins (1999) emphasises that “without a policy, security practices will be developed without clear demarcation of objectives and responsibility”, and David (2002) asserts, “security is not what you do… security is how well you adhere to your formal security policies”.

An effective ISP is therefore an effective tool that organisations, businesses and governments use to ensure the security of their information and information systems. According to Wood (1995), “Policies act as clear statements of management intent and demonstrate that employees should pay attention to information security”.

Security policies differ among organisations depending on critical issues such as the value and sensitivity of the information and technology resources that they protect or want to protect, the potential implications of damage, modification, or disclosure of that information to the organisation (Landoll, 2016; Whitman et al., 2001) among others. To this effect, Baskerville and Siponen (2002) and Whitman (2008) identified three divisions of security policies, and they include the following:

- Enterprise Information Security Policies: This division guides “the development, implementation, and management of the security program, as well as assigns responsibilities for the various areas of security” (Cram et al., 2017).
- Issue-specific security policies: This division addresses “specific areas of technology, such as the use of e-mail, the Internet, or social media; the configuration of employee workstations; use of personal equipment on organisational networks; and prohibitions against hacking or testing organisational security controls” (Cram et al., 2017) among others. The Issue-Specific Security Policies include “the guidelines and procedures (i.e., acceptable use policies) that employees must adhere to in their daily interactions with information and technology resources and describes penalties for non-compliance and other undesirable computing behaviours” (Cram et al., 2017).
- Technical Security Policies (Automated Security Policies): This division relates to “the security architecture of technological systems” (Cram et al., 2017). This division, according to Cram et al. (2017), “combines standards and procedures with the configuration or maintenance of a system”.

Knapp et al. (2009) also acknowledge the reliance of organisations on information systems and attribute this to the reliance of organisations on Information Systems for their operations despite the growing security threats related to such systems. This reliance has, therefore, called for the need to protect organisations' valuable information to provide information security assurance to the people whose personal data is collected and managed.

2.7.1 IS Management

Raggad (2010) defines Information Security Management as ‘accurately identifying all security risks, assessing them and mitigating them by devising a comprehensive risk-driven security program”.

Raggad (2010) advocates for effective Information Security Management to address issues related to information security by “accurately identifying an organisation’s computing environment, defining its criticality and prioritising its contributions to the organisation’s business-value-generation capabilities” (Raggad, 2010).

Generally, the IS principles and management involve using both technical and non-technical approaches to ensure the security of both information and information systems. As Taylor et. al. (2020) noted, “Information assurance is almost entirely about the management of risk”. This is done by adopting and using an Information Security Policy (ISP). Taylor et al., (2020) explain “the inclusion of assurance as part of the operational policy of an organisation is the only cost-effective way of covering the issues adequately”. ISACA (2009) argue that an ISP in the form of an IS program must look beyond technical issues and consider factors such as how the particular institution, its users, processes and adopted technology interact, as well as the impact of culture, humans, and architecture on the institution’s information security management. Due to the acknowledgement of ISPs being an essential tool for information security, many research works have now focused on the factors that influence ISP Compliance. This is due to their importance in ensuring the security of information and information systems. ISPs generally ensure that an organisation implements, enforces, and complies to protect and secure data against attacks. According to Flowerday and Tuyikeze (2016), “One important mechanism for protecting organisations’ assets is the formulation and implementation of an effective Information Security Policy (ISP)”. This means that to protect and secure data against attacks, organisations, institutions, and businesses require an effective Information Security Policy (ISP). Karlsson (2017) indicates that institutions and businesses must consider both the perspectives of management and employees when designing an information security policy to make it more practical and useful for information security management. Further to this, Johnson (2006) also identified the need for organisations to have an information policy that takes into account local information security philosophy and commitments. Samonas et. al. 2020 point out that “more research is required if we are to understand the relationship between the differing perceptions that stakeholders have regarding a security policy and the attitude and behaviour of stakeholders towards policy compliance”.

Additionally, policies aim to provide management direction and support for information security in agreement with business requirements and relevant laws and regulations (ISO/IEC, 2005). Chen and Li (2014) assert that an information security policy is used by management to differentiate between employee behaviours that are either permitted or prohibited, as well as the consequent sanctions if the forbidden behaviours take place.

Organisations have also placed an increasing reliance on security policies, developed in part, to guide employee compliance with external regulations such as the Sarbanes–Oxley (SOX) Act, the Health Insurance Portability and Accountability Act (HIPAA); the Payment Card Industry Data Security Standard (PCI DSS); and the European Union Data Protection Directive (EU DPD); (Kiel et al., 2016; King & Raja, 2012; Koops, 2014; Wall et al., 2015). The reputational, financial, and legal implications of information security incidents have also motivated organisations to implement detailed policies related to topics including access controls and authorisation, data classification, data storage, and virus protection (Siponen, 2006; Spears & Barki, 2010; Wiant, 2005).

The importance of an ISP cannot be underestimated. Some scholars have indicated that ISPs play an integral role in the planning and control context by establishing limits of acceptable behaviour, decision confines, and standards (Davis & Olson, 1985). Von Solms and Von Solms (2004) have emphasised that policies are critical to information systems security as they provide the blueprints for an overall security programme and create a platform to implement secure practices in an organisation.

ISPs also describe ways employees are expected to play a role in assisting their institution in achieving its vision and mission (Höne & Eloff, 2002b). According to Tryfonas et al. (2001) and Canavan (2003), an ISP is a set of rules or requirements that are related to information security and enacted by an organisation to be adhered to by all to protect the confidentiality, integrity and availability of information and other valuable resources from security incidents.

In addition, organisations, institutions, and businesses are encouraged to validate their ISPs well-structured and planned effectively (Von Solms & Von Solms, 2004; Vroom & Von Solms, 2004; Hong et al., 2006; Alnatheer & Nelson, 2009; Ammann & Sowa, 2013; Sommestad et al., 2014).

This means that the individuals, processes, and technology are all needed to achieve adequate security management by developing and implementing an effective ISP to enable effective risk management relative to threats and vulnerabilities to systems and data.

2.7.2 Information Security Governance

The IS governance establishes the organisational structure, frameworks and management strategy. Information Security governance has become more relevant due to the shift towards "soft" indicators of governance and the fact that attention on the "quality of life has increased the demand for information governance as a whole (Liang et al., 2001). Governance refers to steering and has to do with the ability of human institutions to control their societies (Peters, 1995).

Generally, corporate governance focuses on how the board of Directors and executive management manage a company or an institution. The IT governance is concerned with how technology can be used to support business needs and demands. Knapp et al. (2009) argue that "a failure to establish adequate governance prior to developing security policies will likely lead to a less effective process, resulting in diminished organisational security". Taylor et. al, (2020) argue that due to increasing legislations and regulations, senior management of organisations are tasked to ensure that they review, update, and approve their policies and communicate content to both internal and external stakeholders.

According to Raggad (2010), the purpose of IT governance, corporate governance and information security is similar because they share functionality and goals. Even though they have different focuses, the ultimate is to help organisations grow and prosper.

Information Security Governance can, therefore, be defined as a set of tools, personnel and business processes that ensure security is carried out to meet an organisation's specific needs by providing roles, responsibilities, performance measurements and oversight responsibilities (Raggad, 2010).

To Shon Harris (2017), information security governance is "a coherent system of integrated security components (product, personnel, training, processes, policies, etc.) that exist to ensure that the organisation survives and, hopefully, thrives”. Shon Harris (2017) further explains that some of the functions of an Information Security Governance Board of Directors and executive management will include the following:

- Board members understand that information security is critical to the company and demand to be updated quarterly on security performance and breaches.
- The Chief Executive Officer, Chief Finance Officer, Chief Information Officer, and business unit managers participate in a risk management committee that meets each month, and information security is always one topic on the agenda for review.
- Executive management sets an acceptable risk level that is the basis for the company’s security policies and all security activities.
- Executive management holds business unit managers responsible for risk management activities for their specific business units.

Critical business processes are documented along with the risk inherent in the various steps within the business processes.
Employees are held accountable for any security breaches they participate in, maliciously or accidentally.
Security products managed services, and consultants are purchased (hired) and deployed in an informed manner. They are constantly reviewed to ensure they are cost-effective.
The organisation is continuing to review its business processes, including security, to improve continuously.

2.7.3 Effective Information Security Policies

Generally, it is essential to note that the objective of a policy is to provide management direction and support for information security in agreement with business requirements and relevant laws and regulations (ISO/IEC, 2005).

Flowerday and Tuyikeze (2016) suggested, “For an information security policy to survive and attain its objectives, management, employees, and stakeholders need to support the entire process involved in developing and implementing it”. Developing an effective security policy requires a combination of skills emanating from the different stakeholders' experiences (Diver, 2007).

According to Cram et al. (2017), “users of information and technology resources should behave to prevent, detect, and respond to security incidents”.

An information security policy “must be based on relevant risks (i.e. it should be relevant to employees), match the audience’s language, be up-to-date, and have a clear structure” (Karlsson et al., 2017).

It is also vital to ensure an effective ISP formulation, development and review process involving every internal or external stakeholder (Siponen, & Oinas-Kukkonen, 2007).

In addition, the ISP should be compliant, focused, comprehensible, enforceable, and manageable (Dhillon, & Backhouse, 2001).

Information security policies should also involve key issues relative to IS effectiveness, IS management and ISP development, implementation and evolution. Taylor et. al., (2020) acknowledge that the ISPs that ensure IS must be “comprehensive but digestible, pithy, something that can be read easily and something they will actually read”.

An effective ISP should cover all aspects of information security, including physical, technical, and administrative controls (Cram et al., 2017).

Additionally, Ording et al., (2022) advocate that an effective ISP must be enforceable, meaning it should be practical and realistic for the organisation to implement and maintain.

Ording et al., (2022) also advocate that an effective ISP should be regularly reviewed and updated to reflect changes in the business environment, emerging threats, and technological advancements and should align with business goals to achieve overall business objectives and regulatory requirements.

Karlsson et al., (2017) highlight that an effective ISP should recognise and ensure stakeholder involvement in the policy formulation process to ensure that the policy is relevant and understood by those who need to comply with it.

The policy should be written in clear and understandable language to ensure that all employees and the relevant stakeholders can comprehend and follow it (Ording et al., 2022). For instance, A report by PwC shows staff-related breaches in 72% of institutions where security policy was poorly understood (PwC, 2015).

The above highlights that organisations and businesses must have a policy that is well developed, well understood by stakeholders, enforceable and could be quickly reviewed to meet the needs or changes that evolve with time (Cram et. al., 2017, Culot et. al., 2021). Achieving this requires motivating organisations to establish and maintain an effective security policy process to manage and achieve their overall organisational objectives effectively.

2.7.3.1 ISP Development

Whitman et al. (2001) argued that Information Security Policy Development is “the first step toward preparing an organisation against attacks from internal and external sources”. This means that organisations need to develop an ISP to enable them to address their security challenges.

Regarding the ISP development process, two main arguments could be identified from the literature. The first relates to what is required for the development of good policy and the second is on the potential issues that ISP development should aim to avoid. The requirements for the development of the policy focus on issues such as the need for alignment with the organisational aims and objectives, adherence to relevant legislation, involvement of all staff, and language that is understandable by all staff. Wood (1995) provided guidelines for the information security policy design process. The guidelines indicated that different organisations often require tailored policies by stating, “One must understand the special needs of an organisation before one attempts to generate specific written management directives.”

Flowerday and Tuyikeze (2016) suggested, “In order for an information security policy to survive and attain its objectives, management, employees and stakeholders need to support the entire process involved in developing and implementing it”. This is because developing an effective security policy requires a combination of skills emanating from the different stakeholders' experiences (Diver, 2007). In addition, Flowerday and Tuyikeze (2016) suggest involving Management Support and Employee Support in all the processes when developing and implementing an Information Security Policy.

Robinson and McMenemy (2020) state that “users will determine how effective the information security policy is”. This means that the information security policy design should focus on factors that can make it user-focused – from the writing style and the way it is presented to the deployment of the document (Höne and Eloff, 2002). Robinson &

McMenemy (2020) further state that a way to make an ISP like the Acceptable User Policy more user-focused is when the researchers or developers “invite users into the design process”.

Regarding the potential issues that ISP development should aim to avoid, the literature highlights some issues such as the conflict between policy and working practices, references to legislation that staff may not understand, and consistency between documents among others. On this, Adams and Sasse (1999) argued that ISP design could impair employees’ information security behaviour due to how cumbersome and incompatible they are with existing work practices. Karlsson et al. (2017) add that ISP development should address some critical issues about IS management during the development process to ensure clarity. For instance, Karlsson et al. (2017) discovered that the ISP documents analysed recognise that “information security management refers to laws and regulations in general, without specifying exactly which laws and regulations.” (Karlsson et al., 2017). This, in effect, makes it difficult for employees to know the exact laws and regulations relevant to them. Another interesting finding from the literature highlights that “none of the three investigated policy documents contains a definition of “sensitive information” and “business-critical information” (Karlsson et al., 2017).

In addition, the research identified contradictions in policy terminologies. For instance, initial impressions were that technical security controls were irrelevant when formulating an information security policy in the first document. However, reference was made to technical security controls subsequently in the second policy document through the request for password control before authorisation.

The work by Karlsson et al. (2017) also exposes some issues about ISP awareness and understanding as research on effective Acceptable Use Policy, for instance, suggests that there is the need for everyone who gets affected by a policy to be involved in its production (BECTA, 2001, 2009; Höne & Eloff, 2002).

Kwame Adjei (2013) also noted that ISP development should recognise the importance of user empowerment and institutional collaboration where various stakeholders are involved in its development and implementation. This he believes would enable an effective and enhanced general acceptance level during its enforcement.

2.7.3.2 ISP Enforcement

The aim of implementing an effective ISP will be achieved when the users are familiar with its content, and comply with its requirements to prevent attacks. Karlsson et al. (2017) state, "Employees' poor compliance with information security policies is a perennial problem for many organisations". Even though research has further shown that despite information system security policies being in place to protect an organisation against abuse, destruction and misuse, employees generally do not comply with such documents (Vance et al., 2012). There is a need for ISPs to be enforced using multi-faceted strategies. Analysis from the literature highlights that to enhance employee compliance, organisations can adopt several strategies such as the following:

- Sanctions: Deterrence theory literature shows that implementing sanctions for non-compliance can reduce deviant behaviour. Sanctions can include disciplinary actions, fines, suspensions or even termination of employment (Trang & Brendel, 2019). However, the effectiveness of sanctions can vary based on the organisational context and cultural factors (Trang & Brendel, 2019).
- Rewards: The literature also notes that Positive reinforcement through rewards can motivate employees to comply with ISPs. Rewards can be intrinsic or extrinsic in the form of bonuses, recognition, or other incentives that acknowledge compliant behaviour (Woo & Verdier, 2020).
- Protection Motivation Theory (PMT): The literature on PMT explains that individuals are motivated to protect themselves based on their perceptions of threat severity, vulnerability, response efficacy, and self-efficacy (Herath & Rao, 2009). Organisations can therefore enhance compliance by increasing awareness of potential threats and the effectiveness of protective measures, as well as by boosting employees' confidence in their ability to adhere to ISPs (Herath & Rao, 2009).
- Psychological Empowerment: Empowering employees through security education, training, and awareness (SETA) programmes can enhance their intrinsic motivation to comply with ISPs. Providing access to information security strategies and involving employees in decision-making processes can also foster a sense of ownership and responsibility (Abdul Talib & Dhillion, 2015).

By integrating these models, organisations, governments and businesses can create a comprehensive approach to improving ISP compliance among employees, and other stakeholders thereby enhancing ISP enforcement and overall information security.

2.7.3.3 ISP Awareness

Knapp et al. (2009) emphasise that “Organisations train and indoctrinate its members to internalise knowledge and skill that enables the worker to make decisions consistent with organisation objectives”, and this requires the need to provide an organisational awareness programme, which most often, is the “initial phase of a broader security training program”. Straub and Welke (1998) indicate, “Awareness alerts employees to the issues of information security”, and awareness and training is an ongoing process.

Mikuletic et al. (2024) acknowledge that “awareness training is considered an essential means for ensuring proper practical implementations of ethical norms, such as privacy-preserving behaviour”.

As part of ISP Awareness, the successful implementation of a security policy rests on effective communication of prescribed rules to organisational stakeholders (Alraja et. al., 2023). This communication includes having a complete policy but must be “complemented with a thorough understanding of organisational stakeholders' perceptions regarding a security policy” (Niemimaa et al., 2013).

2.7.3.4 ISP Evolution

According to Doherty et al. (2006), “researchers and practitioners are beginning to recognise that the information security policy should relate in some way to corporate objectives”.

According to the International Standard, there should be a review or amendment of information security policy “in response to any changes affecting the basis of the original risk assessment, e.g. significant security incidents, new vulnerabilities or changes to the organisational or technical infrastructures” (ISO 17799, 2000, p. 2)

Doherty et al. (2006) further suggest that ISPs must be “periodically reviewed and modified to ensure that it is pertinent to the organisation's changing needs”. Doherty et. al., (2006) also advise that the ISP review process should not be explicitly integrated into the formulation process.

2.7.3.5 ISP Content

Despite the consensus on the importance of Information Security Policies (ISPs) for organisations and businesses (cf. Baskerville and Siponen, 2002; Herath & Rao, 2009; Höne & Eloff, 2002), there has been limited empirical research on how the content of these policies should be designed (Doherty et al., 2009). Doherty et al. (2009) noted, "Very few studies explicitly address how the scope or content of information security policies support the employee in their daily work. Höne and Eloff (2002) advocate that ISP content should include general characteristics that enhance its communicative effectiveness. These characteristics include being concise and easy to read, reflecting the organisational culture, having a relevant visual appearance, being up-to-date, and being realistic. These elements ensure that the policy is not only understood but also adhered to by employees.

Goel and Chengalur-Smith (2010) also note that the ISP content should recognise the proposed quantitative metrics for assessing the communicative effectiveness of the ISPs by focusing on brevity, breadth, and clarity. In more specific details, Brevity assesses the repetitiveness of words in a document, arguing that "low repetitiveness eliminates redundancy and jargon" (Karlsson et al., 2017). Breadth measures the comprehensiveness of a policy, aligning with Hong et al. (2006)'s suggestion that policies should be as comprehensive as possible. Clarity is evaluated based on readability metrics such as the Flesch Reading Ease Score, Flesch–Kincaid Grade Level, and the Gunning Fog Index.

Other literature works argue that the ISP content should recognise the types of Policies that the organisation wants to develop. This is because different types of ISPs address various aspects of information security. For instance, data protection policies outline measures for safeguarding sensitive information, user access policies define the permissions and restrictions for accessing organisational resources, and incident response policies provide guidelines for handling security breaches. Each type of policy should therefore include specific elements relevant to its purpose, ensuring comprehensive coverage of all security aspects (Cram et al. 2017).

By focusing on key ISP content issues, organisation-specific content requirements and critical issues could be acknowledged and addressed. This would enable organisations to develop policies that are not only effective in theory but also practical and implementable in daily operations.

2.8 Research Gap

The literature highlights that information security is very important for systems such as electronic identity systems and although there is a good understanding in the literature on how information security in organisations should be achieved, it is not clear to what extent existing approaches address the requirements of these systems.

Again, despite the growing importance of Electronic Identity Systems (EIS), there is a notable lack of research specifically addressing the intersection of information security policies (ISPs) and organisational security within EIS contexts. Most existing literature on ISPs tends to focus on general organisational settings or traditional IT systems, without considering the unique socio-technical and legal complexities of EIS (e.g., AlHogail, 2015; Knapp et al., 2009; Siponen & Willison, 2009). While some studies explore broader security concerns such as resilience and ethics in digital identity systems (e.g., Zwitter & Boisse-Despiaux, 2020), comprehensive ISP frameworks tailored to EIS remain underdeveloped.

Additionally, the literature indicates a significant gap in the coverage of perceptions related to electronic identity (eID) services (Lusoli and Miltgen, 2009; Eurobarometer 359, 2011). Understanding citizen perceptions is crucial for the effective design and implementation of these systems, especially given their developmental stage (Kubicek and Noack, 2010).

Moreover, there is a lack of case study research employing mixed methods to assess the effectiveness of IS and ISP in EIS organisations. This gap extends to the absence of literature evaluating the perceptions of both internal and external stakeholders regarding ISPs and employee behaviour towards policy compliance. Furnell et al. (2016) emphasised the need for more research to understand the relationship between stakeholder perceptions of security policies and their compliance attitudes and behaviours.

Samonas et al. (2020) also pointed out the limitation of their study due to the lack of more case studies and historical data from a single organisation, which could be used for comparison and identifying patterns and trends.

It is also clear that information security in organisations is very broad and multifaceted, with information security policies, their development, evolution and management understood to be a key component. However, the literature suggests that to better appreciate the issues surrounding information security policy in organisations, it is important to examine these policies from the perspectives of different stakeholders. For instance, Kwame Adjei's (2013) research on identity systems underscored the importance of user empowerment and institutional collaboration but did not address how to develop effective ISPs that involve various stakeholders in both the development and implementation processes. This gap is critical as stakeholder involvement is essential for achieving organisational objectives and enhancing system, information, user, and service quality.

2.9 Concluding Remarks

The chapter notes that Identity is important for ensuring people's rights and that Electronic identity systems have the potential to address issues with lack of identity for cititheens, so governments are investing in the development of such systems around the world. These systems play an important role in their countries, so ensuring their security, privacy and trustworthiness is crucial.

The chapter also underscores the critical importance of understanding and complying with information security policies (ISPs) for organisations, businesses, and governments. It emphasises that employees of Electronic Identity Systems (EIS) organisations must be particularly vigilant in adhering to these policies to protect the personal data they manage. This vigilance helps prevent potential vulnerabilities and promotes responsible behaviour among employees and other users.

The chapter also highlights that Information security is used by organisations to protect their data and operations. It is broad and multi-faceted covering all aspect from physical security, to network, personnel among others. It explains that Information security policies play a crucial role in ensuring organisational information security. Their effectiveness depends on technical, operational and managerial controls adopted by the organisation as technology alone is insufficient for ensuring information security. Therefore, Social approaches, including human factors and the adoption of motivational and punitive strategies, are essential to supplement technological measures. These strategies can significantly influence compliance with ISPs, benefiting both employers and employees.

Furthermore, although we would expect that information security policies in Electronic Identity systems would have to meet the same criteria, it is not clear whether these are enough to address all their particular requirements. So, research is needed to explore this. Additionally, such research must consider the different stakeholder perspectives to adequately explain the necessity of enhanced security for digitised and digitalised Electronic Identity systems due to their critical functions. As noted in this chapter, it points out the varying relevance of security solutions across different organisations and the need for further research to explore the differences between EIS security and general organisational security.

In addressing the identified research gap, this study focused on the digitised National Identity Authority (NIA) system, acknowledging the broad scope of the gap and the need for targeted research in this area.

The next chapter will discuss the Research Methodology for the research.

3 Research Design and Methodology

In the previous chapter, we identified the lack of comprehensive information security policies tailored to the unique needs of digitised identity systems in Ghana as the area where more research is needed. Specifically, the literature noted that while information security policies (ISPs) are crucial for protecting data and operations within organisations, it remains unclear whether existing ISPs adequately address the specific requirements of Electronic Identity Systems (EIS).

This research aims to explore these gaps, considering the perspectives of various stakeholders to ensure enhanced security for digitised and digitalised EIS due to their critical functions.

In this chapter, we will present the methodology that we followed to address this research gap. This chapter outlines the research aims, objectives, and methodological approaches adopted for this study. It further details the research procedure and justifies both the case study and mixed-method research approaches used.

3.1 Research Procedure

According to Hancock and Algozzine (2016), research procedures are adopted to reach conclusions that are sensible, credible and interpretable by determining the following:

- what we want to study (the research question)
- how do we want to study it (the design)
- whom we want to study (the “case,” “cases,” or “sample”)
- how best to acquire information (the data-collection techniques)
- how best to analyse or interpret the information that we acquire (the data analysis)
- how and with whom to share our findings (the dissemination process)
- how to confirm our findings (the verification process)

Accomplishing this task requires frameworks that “establish for the researcher the defining features and possibilities for acquiring answers to a research question” (Hancock & Algozzine, 2016).

3.2 Research Questions

The research questions guiding this study are:

RQ1: What do information security requirements of identity systems mean to the NIA information security policies?

RQ2: Should NIA ISP be expressed, formulated and implemented differently?

RQ3: What internal and external factors affect the NIA ISP expression, formulation and implementation?

3.3 Justification for the Research Approach

The mixed-method approach combines qualitative and quantitative research, enabling the researcher to leverage the strengths of both methodologies. The flexible nature of mixed methods allows the researcher to use the best qualitative and quantitative techniques to complement and balance the research findings. This approach is particularly suitable for exploring a variety of factors that could influence employee ISP compliance and other relevant aspects.

Contrasting with other approaches, the mixed-method approach provides a comprehensive understanding by integrating diverse perspectives. This considered decision is based on the approach's merits, rather than solely on the literature review.

3.3.1 Why Case Study Approach

The case study approach is chosen for this research based on its ability to provide a complete description of a phenomenon within its context (Hancock & Algozzine, 2016). This method allows for an in-depth exploration of the factors influencing ISP compliance and offers practical recommendations for electronic identity systems management and development. By involving internal and external stakeholders, the case study approach ensures that the findings are relevant and actionable.

Generally, organising frameworks are named by their attributes, and the forms of the attributes are not mutually exclusive in descriptive or inferential research. Descriptive studies involve data collection to describe a specific group without intending to go beyond that group. At the same time, with inferential, the researcher desires to go beyond the group to make generalised statements about a larger population (Hancock & Algozzine, 2016).

Another Organising framework for researchers relates to the level of experimentation. Experimental research involves the manipulation of “independent variables that are combined with random assignment of participants to a group” (Hancock & Algozzine, 2016). On the other hand, quasi-experimental design involves the manipulation of variables but no random assignment of participants. In the case of non-experimental designs, there is no manipulation and no random assignment.

Basic and applied research are other frameworks that researchers use to organise their work. Primary research involves the examination of variables to construct or verify a theory, while applied research primarily addresses an existing problem or issue.

Finally, researchers use qualitative and quantitative research frameworks to plan and conduct their research differently. Quantitative research generally uses numbers to explain phenomena, while qualitative research involves using words to “describe trends or patterns in research settings” (Hancock & Algozzine, 2016).

3.3.2 Justification for Using a Case Study Approach

Overview of Case Study Approach

The case study approach is a non-experimental design that is particularly useful for descriptive and inferential research. It allows for an in-depth examination of a single case or a small number of cases within their real-life context.

Hancock and Algozzine (2010) outline the following as the stages needed for Case Study Research:

- Setting the Stage
- Determining what we know
- Selecting a design
- Gathering Information from Interviews
- Gathering Information from Observations
- Gathering Information from Documents
- Summarising and Interpreting the Information
- Reporting Findings
- Confirmation Case Study Findings

Setting the Stage: This stage involves the identification of a topic for an in-depth analysis in a natural context using multiple sources of information and further determining what is known and unknown about the topic to create a research question (Hancock & Algozzine, 2016).

Determining what we know: This step enables a researcher to establish the conceptual foundation for the study, to define and establish the importance of the researcher's question, strengths, and weaknesses of other researchers' work, focusing on the models and designs used, among others. It also helps researchers identify possible research designs and strategies for their work and how to communicate them to the research community. This determination is done through a literature review.

According to Galvin (1999), literature reviews include the following "directions":

- Select a topic and identify literature to review:
- Identify appropriate databases, review articles, and classic studies.
- Review recent literature first and work backwards.
- Define what is known and what is not known as quickly as possible.
- Analyse the literature:
- Use consistent form for summarising articles.
- Look for strengths and weaknesses.
- Identify gaps in what is known.
- Criticise the literature:

As noted in Chapter 2, it was against the above guidelines that we focused on the literature to establish what was already known and what remains to be known (research gap), which forms the basis for our research.

3.3.2.1 Selecting a Design

According to Hancock and Algozzine (2016), Case Study Designs or approaches are based on the functions, characteristics or disciplinary perspective, and the selection must be based on how well the design allows for a full investigation of a research question.

Yin (2003) indicates that Case study research designs can be classified as explorative, explanatory or descriptive, while Stake (1995) sees case study design as intrinsic, instrumental or collective.

Merriam (2001) categorises case study design as ethnographic, historical, psychological or sociological based on their orientations as detailed below:

- The ethnographic Case Study: It is a design that originates from anthropology, and it is used to "explore the observable and learned patterns of behaviour, customs or ways of life of a culture-sharing group" (Hancock & Algozzine, 2016). It is interesting to note that this research type involves extended interaction with the group, and the researcher immerses himself in the daily lives of the group members.

- Historical Case Study Design: It is used to "often describe events, programs or organisations as they evolve" (Hancock & Algozzine, 2016). It is seen as an extended traditional historical research and includes both direct observation and interviews of key participants. It produces more than a chronological listing of events, resulting in the researcher's descriptive interpretation of factors that cause and result in an event (Hancock & Algozzine, 2016).
- Psychological case study Design: It is used to "examine literature and practices relating to psychological theories and concepts, focusing on the individual and organisations, programmes and events" (Hancock & Algozzine, 2016).
- Sociological Case Study Research: It focuses on society, societal institutions, and social relationships by examining people's structure, development, interactions, and collective behaviour (Hancock & Algozzine, 2016).

3.3.2.2 Instrumental Case Study

It is usually related to case studies that relate to a better understanding of a theoretical question or problem. The three types of Case Study Research Designs are:

- Exploratory: It generally seeks to define the research questions of a subsequent study or determine the feasibility of the research procedures (Hancock & Algozzine, 2016). Exploratory Case Study designs are mainly carried out before an additional research effort through fieldwork and information collection before defining a research question.
- Explanatory: It seeks to establish a cause-and-effect relationship, with the primary focus being how the events occur and "which ones may influence particular outcomes" (Hancock & Algozzine, 2016).
- Descriptive: It attempts "to present a complete description of a phenomenon within a context" (Hancock & Algozzine, 2016).

3.3.2.3 Mixed Methods

The mixed method is a form of research method that combines qualitative and quantitative methods to provide an elaborate understanding of a phenomenon. This research is based on the mixed method due to its benefits.

3.3.2.4 Advantages of Mixed Methods

According to Hurmerinta-Peltomaki and Nummela (2006), mixed methods increase the validity of research findings and inform second data source collection, thereby helping create knowledge. In addition, the authors indicated that the mixed methods approach helps attain a broader and more profound comprehension of the phenomenon than using either a quantitative or qualitative approach.

Some researchers also believe the mixed method approach is more valuable than the qualitative or quantitative methods and receives more citations (Molina-Azorin, 2011).

Mixed methods provide an integration component that gives readers more confidence in the research results and conclusions (O'Cathain et al., 2010).

Mixed methods also help researchers cultivate ideas for future research (O'Cathain et al., 2010).

Some researchers add that mixed-method research provides the only way to confirm findings (Coyle & Williams, 2000; Sieber, 1973) and interpretation (Morse & Chung, 2003; Tashakkori & Teddlie, 2003b).

3.3.2.5 Disadvantages of Mixed Methods

As part of the disadvantages of mixed methods, McKim (2017) states, "Researchers typically require additional funding for added supplies, extra space to interview participants or administer a survey, and assistants to help with data collection and analysis".

Again, McKim (2017) adds that mixed methods research "requires knowledge of both quantitative and qualitative methodology".

In addition to the above, "Many researchers do not have training in quantitative and qualitative methodology; so, this can mean finding additional researchers with expertise in a particular area" McKim (2017).

As part of the design selection and based on our research plan or the nature of our research, we decided on our design, as detailed in this chapter.

3.3.2.6 Relevance to the Current Research

This research is descriptive as it aims to provide a detailed account of the factors influencing ISP compliance within the context of the Ghanaian National Identity System. A non-experimental design is appropriate because it allows for the exploration of these factors without manipulating the study environment.

3.3.2.7 Frameworks and Positioning

In the context of different research frameworks, this study stands as a descriptive case study. The choice of a case study approach is justified by its ability to provide rich, contextual insights that are not easily achievable through other research designs. This approach is particularly relevant for understanding complex phenomena such as ISP compliance in digitised identity systems.

3.3.3 Implementation of the Case Study

To implement the case study, we adopted a mixed-method approach. This combination allows us to gather comprehensive data and insights, enhancing the value of the research findings. The mixed-method approach complements the case study by providing both qualitative and quantitative data, ensuring a balanced and thorough analysis.

3.4 Study Aims and Objectives

The research generally sought to achieve the following objectives:

- Examine a particular case study (in this case, the Ghanaian Identity System ISP) to concretely examine the topic and make recommendations that can be practical and potentially make a difference in the formulation and implementation of Electronic Identity Systems.
- Aim to establish whether and how Information Security Policies in Identity Management should differ from those of other organisations.
- Intensively describe and analyse the various stages the Ghanaian Identification Authority Information Security Policy (GIA-ISP) was formulated and implemented.
- Understand the role of stakeholders in the formulation, development, and implementation of the GIA-ISP and its effectiveness.

We conducted four studies to achieve these objectives based on the research gap identified. These four studies come together to answer our research objectives and questions. Studies 1 and 2 give us insights from the internal stakeholders' perspective about their involvement and perception in the development, compliance, enforcement and evolution process, while studies 3 and 4 give insights into the involvement and perception of external stakeholders in the development, compliance, enforcement and evolution process. The four studies included two survey questionnaires and two interviews, as detailed below:

- Study 1: NIA Internal Stakeholders Survey focused on Junior and Middle employees
- Study 2: NIA Management Interviews
- Study 3: NIA External Stakeholders Interviews
- Study 4: General Public Survey

The survey questionnaires were paper-based and were manually distributed to the participants in the two survey studies.

In the case of the two interviews, we used a semi-structured interview guide to get tentative responses from the NIA Management and external organisations management members to probe further when needed. This aligns with the findings that semi-structured interviews help "to ask predetermined but flexibly worded questions, the answers to which provide tentative answers to the researcher's questions" (Hancock & Algozzine, 2016). Semi-structured interviews further enable follow-up questions to probe into issues of interest to the interviewees (Hancock & Algozzine, 2016).

3.5 The NIA

The NIA was established in 2003 with the mandate to issue national ID cards to citizens and residents and manage the National Identification System (NIS). The NIA operates in four zonal operational regions in Ghana to carry out its mandate effectively. The Head office is in Greater Accra, with the Ashanti regional office in Kumasi, the Northern regional office in Tamale and the Bono regional office in Sunyani. The Ghanaian Identification System is digitised, where citizens' and residents' personal data are collected and stored. The applicants are issued a smart card to prove their identity when accessing essential services like mobile phone Subscriber Identity Module (SIM) card registration and banking services. Currently, the NIA is issuing biometric identity cards throughout the country. While this is ongoing, telecommunication companies and banking institutions must legally reregister all customers by demanding a national ID card as proof of identity. Protecting collected citizens' data is an essential part of the NIA mission. The NIA management recognised the importance of securing the NIS from the outset. It developed a formally approved information security policy (ISP) and introduced formal ISP awareness training for all staff to boost ISP compliance. More recently, NIA management updated the ISP to match international standards, and a revised policy was drafted. However, the revised policy was never formally approved, while formal ISP awareness staff training was suspended until the formal approval. In the meantime, the NIA has been growing, with many staff being hired in recent years. Moreover, in collaboration with a private company, the NIA is conducting a nationwide identity registration exercise to ensure that all citizens and residents are issued national identity cards. This means that additional staff have been contracted to register the population.

The public-private partnership is an official arrangement between the government, which acts on behalf of the NIA, and a private company, the Integrated Margins Group (IMS), to ensure the management of the NIS and the issuance of biometric cards to citizens and residents. Although the employees' line managers make new staff aware of ISP compliance expectations, they have not had the clarity of a formal ISP and have not benefited from any awareness training. The current situation concerning new staff and the ISP raises concerns about compliance in light of the personal data that NIS manages. This situation is concerning for the security of citizens' and residents' data, making the NIA an exciting case study to investigate its staff perceptions and the reality of its ISP awareness, the level of involvement of the external stakeholders in ISP formulation, development and implementation and how the NIA handles its information security requirements as contained in their ISP. The internal stakeholders are the internal employees be they Junior, middle or management members of the NIA who collectively contribute to the administration and management of the organisation to achieve the organisational objectives. The external stakeholders are the user agencies that rely on the NIA system for services such as identification, authentication, and verification of their customers. The diagram below shows the NIA and its relationship with both external and internal stakeholders using a process flow chart:

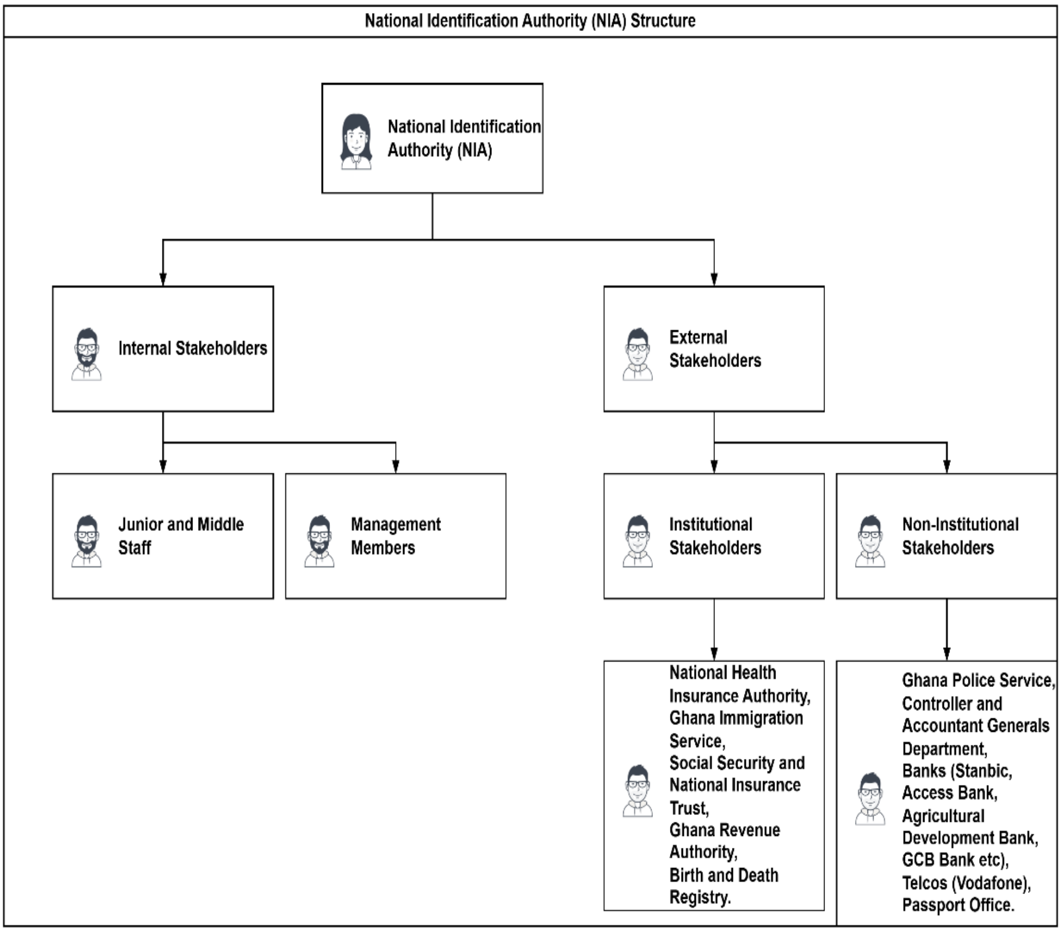

National Identification Authority (NIA) Structure
National Identification Authority (NIA)
Internal Stakeholders
External Stakeholders
Junior and Middle Staff
Management Members
Institutional Stakeholders
Non-Institutional Stakeholders
National Health Insurance Authority, Ghana Immigration Service, Social Security and National Insurance Trust, Ghana Revenue Authority, Birth and Death Registry.
Ghana Police Service, Controller and Accountant Generals Department, Banks (Stanbic, Access Bank, Agricultural Development Bank, GCB Bank etc), Telcos (Vodafone), Passport Office.

Figure 2: NIA and its relationship with internal and external stakeholders

3.6 Interviews

After we identified our disciplinary orientation and design for the research, we realised that gathering information to address the research question(s) was necessary and decided to interview the general participants for our two studies (see the chapters 5 and 6 data collection sections for more details). This is because the widespread use of interviews to gather information in case study research allows the researcher to "attain rich, personalised information" (Mason, 2002).

According to Hancock and Algozzine (2016), a researcher must follow the guidelines below when using an interview approach:

First, the researcher must identify key participants whose knowledge and opinions may provide insights to address the research questions to prevent wasting time.

Secondly, the researcher should develop an interview guide (called interview protocol) to identify appropriate open-ended questions. The open-ended questions enable the researcher to “gain insights into the study’s fundamental research questions; hence, the quantity of interview questions for a particular interview varies widely” (Hancock & Algozzine, 2016).

Again, the researcher should consider the setting in which the interview is conducted. Hancock and Algozzine (2016) indicate that, even though interviews in natural settings enhance realism, researchers can “seek a private, neutral, and distraction-free interview location to increase the comfort of the interviewee and the likelihood of attaining high-quality information”.

The fourth guideline is where a researcher is supposed to develop a means of recording the interview data. According to Hancock and Algozzine (2016), the best way to do this is to audiotape the interaction to prevent valuable data loss associated with handwritten notes. It is, however, necessary to seek the participant’s permission before you proceed to audiotape. After the interview, the researcher transcribes the information for closer scrutiny and comparison with data obtained from other sources.

Finally, the researcher must adhere to legal and ethical requirements for all research involving people. Interviewees should not be deceived and should be protected from mental, physical, or emotional injury. The interviewees are also to provide informed consent for their participation in the research. Again, information obtained from interviews must be confidential and anonymous unless otherwise required by law or the interviewee's consent to public identification. Interviewees also have the right to end the interview and should be debriefed by the case study researcher after the research has ended (Hancock & Algozzine, 2016).

3.6.1 Forms of Interviews

Interviews may be structured, semi-structured or unstructured.

Semi-structured interviews are particularly well suited for case study research. This is because researchers can "ask predetermined but flexibly worded questions, the answers to which provide tentative answers to the researcher’s questions” (Hancock & Algozzine, 2016). Semi-structured interviews further enable follow-up questions to probe issues of interest to the interviewees (Hancock & Algozzine, 2016).

3.6.2 Identifying Interviewees

The selection of interviewees directly influences the quality of information to be obtained, so there is the need to use specific parameters or identifiers to get the right people. According to Hancock and Algozzine (2016), the most crucial consideration in selecting interviewees is identifying persons with the best information to address the research questions and availability. The researcher is also supposed to have the ability and resources to gain access to the interviewees.

Taking Glassner and Moreno's (2013) advice on using qualitative methods for the best benefit in areas with little or no existing knowledge, we decided to do an interview approach to realise our objective. To this effect, we designed a semi-structured interview guide to solicit the views of the NIA's senior staff and the NIA's external stakeholders about their awareness, actual knowledge and understanding of ISP provisions in the context of EIS ISP provisions. The interview guide also focused on the importance and concerns of Information Security and its Management. It also focused on the ISPs' development, implementation, and evolution relative to compliance and enforcement. This was to intensively describe and analyse the various stages used in formulating and implementing the NIA’s Information Security Policy in the context of EIS and to ascertain the respondents’ views on the Information Security Effectiveness, Information Security Management, and Information Security Policy of the NIA. We interviewed nine (9) senior members of the NIA for the senior management study and in the case of the external stakeholders' study, we interviewed 14 of them to assess their involvement in the formulation and implementation processes of the ISP.

After the interviews, we then transcribed them and used the NVIVO software for further analysis. Using the NVIVO software, we coded the responses into themes for further analysis.

3.6.3 Summarising and Interpreting the Information

The essence of Case Study research is to make sense of information collected from multiple sources. According to Hancock and Algozzine (2016), information collected from multiple sources is a recursive process in which the researcher interacts with the information throughout the investigative process to make sense of it. Case study research “involves ongoing examination and interpretation of data to reach tentative conclusions and refine research questions” (Hancock & Algozzine, 2016).

To do a better summary and interpretation, a Case study researcher adheres to several guidelines as indicated below:

First, the researcher is required to continuously refine the study’s fundamental research questions in the light of the data obtained early in his/her investigation (Hancock & Algozzine, 2016)

Again, there should be a constant focus on the research questions being investigated despite the overwhelming data obtained through interviews, observations and documents (Hancock & Algozzine, 2016).

Thirdly, the researcher is to collect and interpret only data that are “potentially meaningful to his/her research effort” (Hancock & Algozzine, 2016). Here, the researcher is required not to eliminate information prematurely, nor is he/she encouraged to keep irrelevant information.

Another guideline is for the researcher “to develop a method for labelling, storing and gaining access to information acquired during the research effort” (Hancock & Algozzine, 2016). Hancock and Algozzine (2016) further indicate that “at minimum, every information gathered must be labelled with the date, location, person involved and circumstances surrounding the collection of that information”.

Finally, there is the need for the “use of all available resources that can assist in the collection and interpretation of information” (Hancock & Algozzine, 2016). For instance, NUDIST and Ethnography software can help categorise and process large amounts of information (Hancock & Algozzine, 2016).

More importantly, due to the need for these guidelines, a case study researcher adjusts his research questions and methods based on when information becomes available for analysis. At the same time, “the researcher makes every effort to keep fundamental research questions at the forefront of the investigative process” (Hancock & Algozzine, 2016).

3.6.4 Reporting Findings

A researcher's work synthesises the information acquired during research to identify and report meaningful findings (Hancock & Algozzine, 2016). To carry out this function, researchers develop strategies such as thematic analysis, categorical analysis, and narrative analysis to accomplish the task of case study research.

According to Hancock and Algozzine (2016), strategies have unique characteristics despite having a standard process. Some common processes they share include repetitiveness and ongoing review of accumulated information to “identify recurrent patterns, themes or categories”.

A critical endeavour of a case study researcher is to determine information–supported themes that address a research question using criteria that “accurately and comprehensively represent the information collected in the study” (Hancock & Algozzine, 2016). This can be achieved when the themes reflect the research's purpose and respond to the questions under investigation. Again, the theme also evolves from a saturation of the collected information (Hancock & Algozzine, 2016).

Another feature of the theme is that novice researchers should seek to develop themes that represent separate and distinct categories of findings despite their hierarchical and interconnected features (Hancock & Algozzine, 2016).

In addition, the theme needs to be made more specific and explanatory as much as possible or as allowed by the data for the researcher to carry out his work (Hancock & Algozzine, 2016).

Finally, the themes should “be of comparable complexity” (Hancock & Algozzine, 2016).

In writing a case study report, there is no universally accepted format. However, Hancock and Algozzine (2016) indicate that specific components are found in most programmes and activities under investigation and that the research effort is bounded by time and space.

Again, the researcher is supposed to explain his or her relationship to what is being researched and any personal biases brought to the research setting. At the same time, the “research report should reflect the literature related to the topic under investigation and how that literature informs the research question” (Hancock & Algozzine, 2016).

Other factors like disciplinary orientation, the research design of the study and how they influence the information-gathering strategies used must also be addressed (Hancock & Algozzine, 2016). The research report must include information collection strategies such as interviews, observation, and document reviews and “must be richly descriptive and include key participants’ statements that elucidate significant findings” (Hancock & Algozzine, 2016).

Finally, Hancock and Algozzine (2016) indicate that the strategies for interpreting, reporting, and confirming the research findings should be well articulated.

3.6.5 How to Synthesise Findings

Case Study research generates large amounts of information from different sources and needs to be synthesised by "combining, integrating and summarising findings" (Hancock & Algozzine, 2016). According to Hancock and Algozzine (2016), answering the following questions can facilitate the process of synthesising information:

- What information from different sources goes together?
- Within a source, what information can be grouped?
- What arguments contribute to grouping Information?
- What entities bounded by space and time are shared?
- How do various sources of information affect findings?
- What information links various findings together?
- What previous work provides a basis for analysis?
- What questions are being answered?
- What generalisations can be made?

Alternatively, the synthesisation of the information can be done and presented using the sources that provide the information, such as people, places, things, events, organisations or documents (Hancock & Algozzine, 2016).

3.6.6 Confirming Case Study Findings

A Case Study researcher must confirm the study's findings before disseminating the final report. The findings are confirmed once information is gathered, synthesised and reported by the researcher (Hancock & Algozzine, 2016).

Some of the strategies used to confirm the findings of a case study research work, even though the researcher is required to use as many as he/she can, include the following:

First, Sharing the results with those examined for the study extends the "intent of the researcher's ethical obligations to debrief participants in the study" (Hancock & Algozzine, 2016) and further allows for feedback to be received from the participants. The feedback allows the researcher to gain perceptions of the plausibility of the findings from the participants' perspective (Hancock & Algozzine, 2016).

Again, a review of the report by fellow case study researchers familiar with the goals and procedures of case study research is another strategy that can be of immense benefit. The case study colleagues "should systematically and thoroughly critique the study's procedures and findings to identify the discrepancies that may threaten the credibility of the research efforts" (Hancock & Algozzine, 2016).

Another strategy is to solicit expert scrutiny of the final report on the topic under investigation to ensure accuracy, clarity and meaning (Hancock & Algozzine, 2016).

A case study researcher can also acknowledge and articulate "personal biases brought to the situation and how he/she attempted to mitigate the potential effects of those biases" (Hancock & Algozzine, 2016). This lessens the likelihood of the researcher being accused of producing contrived findings.

The fifth strategy is to "demonstrate how findings are based on information acquired from multiple sources, sometimes called triangulation" (Hancock & Algozzine, 2016). This is where findings from interviews, observations and documents become more convincing than just one or two sources.

3.6.7 Disseminating Case Study Research

There are several ways that Case Study researchers use to disseminate their research findings to benefit others. However, communicating with colleagues and other stakeholders at professional conferences and through publication in scholarly journals are two common ways of disseminating case study research (Hancock & Algozzine, 2016).

According to Hancock and Algozzine (2016), reports presented at conferences or published in journals include a thorough presentation of the study's findings and a discussion of what the findings mean.

Some suggestions on how to write formal reports in scholarly journals are as follows:

First, case study writers must pay particular attention to the expectations of the journal and its editors because the styles and formats of the journal articles are different from one journal to the other (Hancock & Algozzine, 2016).

Again, the article's introduction must contain the research's purpose, worth and need. This means that the introduction should describe what is known about the topic under investigation, why the study was necessary, what was intended to be accomplished and why the outcome was important (Hancock & Algozzine, 2016).

On methods, it describes in detail how the study was conducted (APA, 2001) by starting with the overview of the method used. To Hancock and Algozzine (2016), the case study researcher can also use a list of questions or sentences to outline the purpose and objectives before providing a formal description. The goal is to provide essential information that helps readers and other researchers understand the study by evaluating the appropriateness and integrity of the work done and the credibility of the outcome (Hancock & Algozzine, 2016).

The study's results summarise the information collected and how it addresses the case study research questions by providing the primary outcome and sufficient details to justify the conclusions regarding primary and secondary questions (APA, 2001).

In discussion, the researcher ties the outcome of the research to the literature and further takes the reader beyond the facts to the meanings they reflect, questions raised, the ideas to which they point and the practical uses and value they have for the extension of knowledge (Hancock & Algozzine, 2016).

Finally, there is also the need for the researcher not to overemphasise limitations and not to generalise beyond the study's outcome by making sure that speculations are identified as such and logically related to the information collected or theory discussed in the study (APA, 2001).

3.7 Survey

The term ‘survey’ refers to research conducted using a representative sample size (Pickard, 2013). According to Schutt (2018), a survey is ideal for collecting data from individuals with different social backgrounds. The survey instrument provides advantages and is considered one of the easiest methods to code closed-ended items (De Leeuw et. al., 2012; Nardi, 2018). According to Kelley et al. (2003), a researcher should follow a “checklist of good practice in the conduct and reporting” to achieve a credible and high-standard survey outcome. Kelley et al. (2003) explain that the step-by-step survey process includes data collection, analysis, and reporting.

The survey method is ideal for our two studies as it can address many samples quickly and at a moderate expense. According to Briggs et al. (2012), the survey method is one of the most widely used research approaches. It is the most employed quantitative strategy due to its distinct advantage over the other methods.

The survey studies were devised and deployed using the Qualtrics survey platform (Qualtrics, 2017). This was because it met our requirements for administering and managing the questionnaire questions (see the chapters 4 and 7 data collection sections for more details).

3.7.1 Forms of Survey Research

Survey research could be descriptive, Analytical or evaluative.

Descriptive research was the most appropriate for our research. This is because it enables researchers "to observe (gather information on) certain phenomena, typically at a single point in time" (Kelley et al., 2003). Kelley et al. (2003) explain that "the aim is to examine a situation, such as demographic, socio-economic, and health characteristics, events, behaviours, attitudes, experiences and knowledge".

Advantages and Disadvantages of Survey Research

According to Kelley et al. (2003), the following are the advantages of Survey research:

- The research produces real-world observation data
- The breadth of coverage provides a basis for obtaining a representative data sample that can be generalisable to a population.
- Surveys help produce large and less expensive data within a short time frame, helping in the planning and timely delivery of research outcomes.

In terms of the disadvantages, Kelley et al. (2003) indicated the following:

- Data significance can be neglected when the researcher is in the coverage range instead of relevant issues, problems or theories.
- The produced data can likely lack details or depth of the investigated topic.
- At times, securing a high survey response rate control becomes difficult.

3.7.2 Identifying Participants (Sample and Sampling)

This is where the researcher decides how to recruit participants for the research and how to select them. Two main types of sampling are Random sampling and non-random sampling. Random sampling uses quantitative methods like questionnaires to collect data, while non-random sampling uses qualitative methods like interviews or focus groups.

In our case, we adopted random sampling for our survey research studies.

3.7.3 Data Collection

According to Kelley et al. (2003), the researcher should be rigorous and ethical and must record the following for a good data collection process:

- How, where, how many times and by whom were potential respondents contacted?
- How many people were approached, and how many agreed to participate?
- How do those who agreed differ from those who refused to participate regarding characteristics such as gender, age, etc?
- How the survey was administered.
- What the response rate was.

3.7.4 Data Analysis

Data analysis aims to summarise data for easy understanding and provide answers to the original questions (Kelley et al., 2003). In addition, Wright et al. (2003) advise that data analysis should help the researcher spend substantial time generating accurate results and conclusions.

3.7.5 Reporting

According to Kelley et al. (2003), a survey researcher must provide a comprehensive report that covers key points such as the following:

- Explaining the purpose or aims of the research, including the research questions
- Explaining the necessity of the research and its context using relevant literature
- Describe how the research was done, including the research methods, justification, and tools.
- Describing the sample, participants' recruitment process, consent approval process, how data was collected and the response rate
- Describing and justifying methods and tests used for data analysis
- Presenting the research results in a clear, factual and concise manner.
- Interpreting and discussing the findings
- Presenting conclusions and recommendations

3.8 Research Question

Bell (1984) indicates that every approach has its strengths and weaknesses, that each approach is likely to be particularly suitable for a particular context and that the choice of which approach to use is based on the research problem and what the researcher is seeking. To this end and for this research, we proposed and chose to find answers to the following broad research questions based on our research objectives:

> **RQ1:** What do the information security requirements of identity systems mean to the NIA information security policies?
>
> **RQ2:** Should NIA ISP be expressed, formulated and implemented differently?
>
> **RQ3:** What internal and external factors affect the NIA ISP expression, formulation and implementation?

We believe the answers to these broad research questions could help fill some of the research gaps identified in the previous chapter and meet our research objectives.

To achieve this, we sought to narrow down the research questions based on the aims and objectives of each study, the nature or type of study and the context of our study. For instance, in the survey research with the NIA junior and middle staff, we sought to answer the following research questions:

- What are the attitudes of NIA staff towards ISP compliance?
- What are their perceptions of the intrinsic and extrinsic rewards for ISP compliance?
- Does experience affect ISP compliance attitudes and reward perceptions of NIA staff?
- Do EIS staff believe they know the rules, regulations, and responsibilities prescribed by their organisation's ISP?
- Do EIS staff appreciate critical provisions of their organisation’s ISP?

Generally, the four studies come together to answer our research questions that focus on how the NIA ISP impacts the lives of employees, residents and citizens regarding Privacy, Trustworthiness, Confidentiality, Integrity, Availability, ISP development, evolution and compliance, among others. However, the different studies address the same questions from different perspectives.

3.9 Survey Study Design

For the surveys, they focused on assessing the extent of awareness, understanding, involvement and compliance of Junior and Middle staff of NIA to their ISP and the public, so we designed a questionnaire for each study with some adapted questions from authors including Bulgurcu et al. (2010), Adele Da Veiga (2018), and Siponen and Vance (2010) and adopted the 7-point Likert scale. We adapted the original questions to conform to our needs to measure the respondents' attitudes effectively. This aligns with some literature and recommendations highlighting that people's attitudes can be measured (Thurstone & Chave, 1929; Desselle, 2005; Likert, 1932). In addition, the questions were validated in previous works by the authors from whom we adopted them.

We also adapted the scales to a 7-point Likert scale to meet our needs for the NIA ISP development and evolution process. The Likert scale was used to assess the respondent's level of agreement with the survey questions, and its values are as follows:

1. Strongly agree
2. Agree
3. Somewhat agree
4. Neither agree nor disagree
5. Somewhat Disagree
6. Disagree
7. Strongly Disagree

Adapting the 7-point Likert scale aligns with suggestions by Willits et al. (2016) and Ifinido (2012). According to Willits (2016), Likert scales allow that “the responses are then scored from 1 to 5 (or 5 to 1) for each item, thus assuming the intervals between responses are equal” and that “Extending the number of categories allows for greater differentiation in responses”. To Ifinedo (2012), the 7-point Likert scale ranging from “strongly disagree” (1) to “strongly agree” (7) helps respondents to indicate the appropriateness of their response. Willits (2016) adds that the Likert scale prevents response-set bias because it allows “A balance of both positive and negative items is generally recommended to reduce response-set bias”. Willits (2016) further recommends, "A seven-category response scale is straightforward and allows for greater differentiation”.

3.10 Interview Study Design

To answer the research questions in the context of EIS from the senior management and the external organisational stakeholders' perspectives, we designed a semi-structured interview guide that focused on the importance and concerns about Information Security and its Management, ISP development, implementation and evolution relative to compliance and enforcement.

More specifically, we posed questions that elicited responses to ascertain their views on the general effectiveness of the NIA's Information Security Management and Information Security Policy from the viewpoint of the senior management and the external stakeholders.

3.11 Participants and Study Procedures

The participants and the study procedures are discussed in this section.

3.11.1 Participants

Study 1:

The survey study involved the distribution of paper-based Questionnaires, which were manually distributed to the Middle and Junior Staff of the NIA throughout the four zonal operational regions in Ghana. The focus of the study was on employees of the NIA. The questionnaire distribution for the employees was done between 14/02/2020 and 20/10/2020 due to the Covid-19 restrictions. We distributed the questionnaire based on the distribution formula. The distribution formula was developed primarily based on the actual staff strength of each unit or department in the various operational zones or offices. This was to ensure fair participation from each unit or department.

To this effect, we distributed 150 questionnaires manually to the employees. We manually collected the results of the self-administered questionnaire, which were later entered into Qualtrics for ease of analysis and used SPSS software for further analysis. The manual data collection ensured easy access to participants and helped prevent the risk associated with unstable internet connectivity in the regions where we collected the data. On average, it took participants about 35 minutes to complete a questionnaire. The questionnaires were manually given to each participant in his/her office to complete independently. Upon completion, the researcher collected them on the same day. This was done to prevent the probability of other participants from influencing other responses when they were grouped.

Study 2

We developed a semi-structured interview guide to enable us to ask the required uniform questions and get the correct responses from participants about their involvement in the development, awareness, evolution and enforcement of the NIA ISP and general information security.

The interview session was face-to-face, and each of the nine participants lasted at least 45 minutes. After the interviews, we transcribed them with the "Temi" software and used the NVIVO software for further analysis. Using the NVIVO software, we coded the responses into themes. After the themes, we interpreted our findings using available tools to make more meanings.

Study 3

We used a semi-structured interview guide to ask uniform questions of participants through an interview session about their relationship and involvement in the development, evolution, and enforcement of the NIA ISP.

The interview session was on a face-to-face basis in their organisations in Ghana. The session lasted a minimum of an hour for each participant and was recorded. After the interviews, we then transcribed them using "Temi" software. We then used the NVIVO software for further analysis. Using the NVIVO software, we coded the responses into themes (Braun & Clarke, 2006). After that, we interpreted our findings using available tools to make more meanings.

Study 4

This study involved the manual distribution of 200 Questionnaires to members of the general public to access and participate in the data collection. The distribution was conducted between 10/01/2022 and 17/02/2022. We conducted the data collection exercise throughout the four operational regions of the NIA in Ghana, including the Greater Accra, the Ashanti Region, the Northern Region, and the Bono Region, by ensuring fair participation from various parts of the country by using a distribution formula that was primarily developed based on the regional population distribution of the country.

We received 155 responses from participants. Out of the 155, we excluded seventeen (17) responses during the data quality checks and analysis because they were incomplete. We collected the results of the self-administered questionnaire and entered them into Qualtrics for ease of analysis. After that, we used SPSS software for further analysis.

3.11.2 Questionnaire Analysis

We categorised the Likert scale as an interval scale with an equal distance between each anchor. This conforms to Stevens' measurement framework, where Likert scale items are summed, averaged, and presented horizontally (Uebersax, 2006). Again, according to Dehaene et al. (1990, 1993), Zorzi et al. (2002) and Cohen et al. (2011), human beings are more comfortable with numerical data than verbal forms of data. Additionally, recent investigations indicate that when people are "presented with numbers, in either numeric or verbal form or relative magnitude, humans have a mental representation of numbers that seems to resemble a mental number line" (Spencer et al., 2015). In furtherance to this, we first entered the questionnaire responses into qualtrics for primary analyses. The data was then imported and stored into the SPSS/PC statistical package for further statistical analysis. These data analysis activities are in furtherance to Babbies' (2016) advice of presenting quantitative descriptions in a manageable form by describing the features of the data in a study. According to Holbert (2013), this type of statistics helps to highlight how "variables are collected" and reflects readily on the responses by the participants. According to Gray (2013), descriptive statistics can describe the basic features of research using graphical analysis.

Qualtrics

According to Cushman et al. (2021), "Qualtrics software, a digital tool used for survey data collection and analysis, has become a commonly used technology in organisations around the country". According to Cushman et al. (2021), the software has been used to:

- create customised evaluation instruments
- improve data collection efficiencies,
- increase quantitative data analysis capacity

We used this software to create customised instruments to match our manual questionnaire. We then transferred the participant's responses into the Qualtrics software and used the software to do fundamental quantitative data analysis. We subsequently decided to do more advanced analyses with the data. To do this requires more advanced statistical assessment knowledge to synthesise and analyse the data, so we transferred the data into the SPSS for further analysis.

SPSS

SPSS (Statistical Package for the Social Sciences) is “a widely used program for statistical analysis in social science” (Jyoti, 2016). According to Jyoti (2016), SPSS is “used by market researchers, health researchers, survey companies, government, education researchers, marketing organisations, data miners, and others”. The software “enables the researchers to obtain statistics ranging from simple descriptive numbers to complex analyses of multivariate matrices along with plotting the data in histograms, scatter plots, and other ways” (Jyoti, 2016).

3.11.3 Quantitative Analysis Methods

The quantitative analysis method involves using organised questions that include prearranged response choices for many participants to administer, and the data produced are usually numerical (Neuman, 2013). The results are generally for a large sample size; therefore, the result can be generalised to a larger population (Scandura & Williams, 2000). We used the quantitative analysis to elicit responses on the NIA junior and middle staff's knowledge, understanding and compliance levels. We also used it to evaluate the attitudes, trust perceptions and expectations of members of the public about NIA staff (see the Chapters 4 and 7 data analysis sections for more details).

3.11.4 Interview Analysis Methods

In our qualitative research, we used an audio recorder to record the interviews with the management and external stakeholders after they consented. Merriam and Tisdell (2016) stated, “In education, if not in most applied fields, interviewing is probably the most common form of data collection in qualitative studies. In some studies, it is the only source of data”.

We interviewed the participants to understand better the perceptions, involvement, and understanding of the NIA management and their external stakeholders about the NIA ISP process. After the interview, we used the “Temi” software to transcribe audio to text.

Guidelines for interview data analysis

To analyse the data from the interviews, the researcher followed the recommendations by Braun and Clarke (2006) guidelines for interview data analysis. The following are the steps used for the two interview data analyses:

- **Transcription:** The researcher transcribed the interviews verbatim using the Temi software by capturing all spoken words and noting non-verbal cues where possible as recommended.

- **Familiarisation:** The researcher immersed himself in the data by reading and re-reading the transcripts to gain a comprehensive understanding of the content.
- **Coding:** After the familiarisation, the researcher adopted a coding process (aided by the NVIVO software) to help identify significant patterns in the data through the inductive process and coded them. This is in line with Braun and Clarke's (2006) recommended guidelines on how the data could be coded.
- **Thematic Analysis:** After the coding, the researcher adopted the thematic analysis process recommended by Braun and Clarke (2006) to identify, analyse, and report patterns within the data. This involved organising the codes into broader sub-themes, themes and categories.
- **Validation:** After the identification of the sub-themes, themes and categories, the researcher cross-checked the codes, sub-themes, themes and categories using a more experienced researcher (the researcher's supervisor). This was to ensure the reliability and validity of the analysis as recommended by Braun and Clarke (2006).
- **Interpretation:** The researcher decided to interpret the sub-themes, themes and categories based on the study's research questions and objectives as well linking the findings to existing literature as suggested by Braun and Clarke (2006).

TEMI

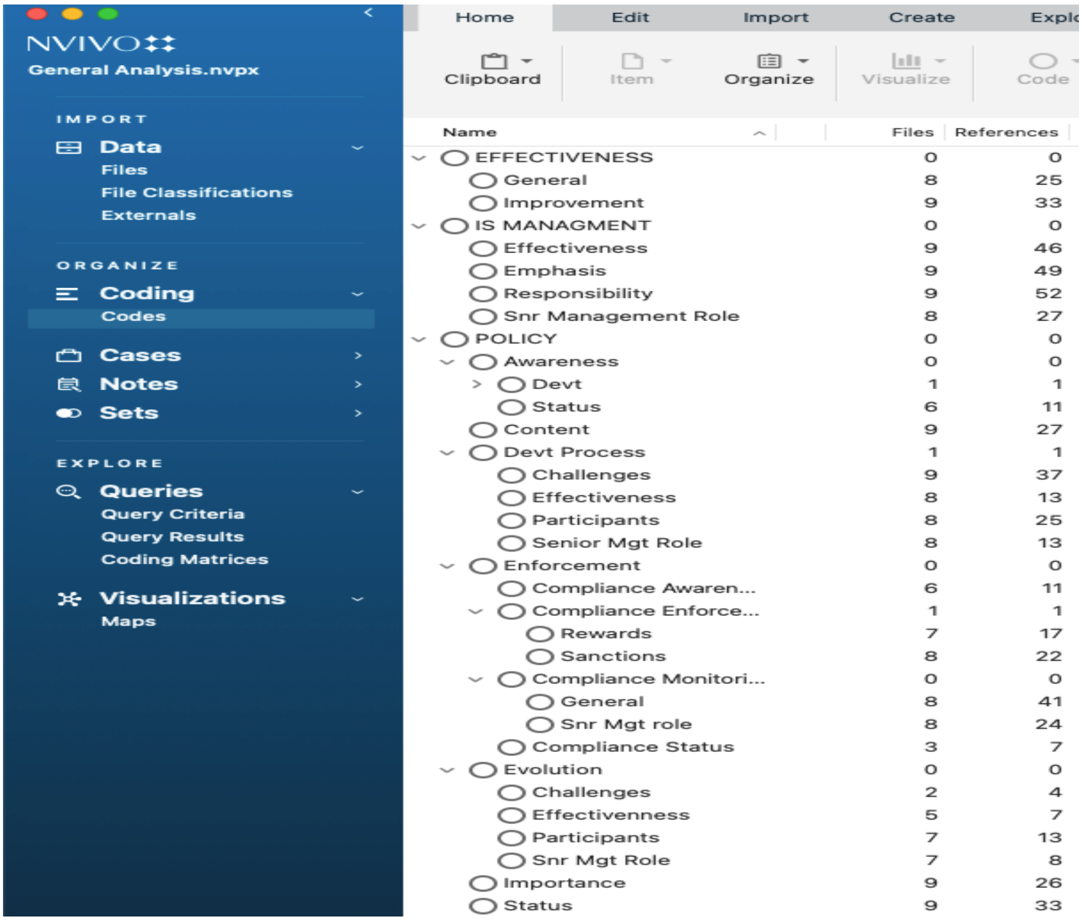
This online transcription software changes audio to text. It also enables the researcher to play the audio while correcting the text regularly to ensure accuracy by matching the text against the audio. After the transcription, the audio files were loaded into the NVIVO software for further analysis.

NVIVO

Qualitative researchers face high volumes of data, making it difficult to manage them manually. As a result, qualitative theorists have encouraged the use of qualitative data analysis software packages (e.g., Berg, 2001; Denzin & Lincoln, 1998; Kelle, 1997a, 1997b; Krueger, 1998; Miles & Huberman, 1994; Morse & Richards, 2002; Patton, 2002; Silverman, 2000, 2001; Taylor & Bogdan, 1998; Tesch, 1990). To this effect, some qualitative researchers have resorted to using NVIVO software for the research work. The Nvivo is a qualitative software researchers use for analysing and managing data. According to Azeem et al. (2012), "One of the most advanced data analysis packages, computer-assisted qualitative data analysis software (CAQDAS) NUD*IST VIVO or NVIVO helps tremendously from conceptualisation and coding of data to an entire research project”. NVIVO also enables the researcher to manipulate data records, browse them, code them, annotate them, and gain access to data records quickly and accurately (Richards, 1999).

According to Welsh (2002), computer-assisted qualitative data analysis enables researchers to analyse data efficiently because coding is done more quickly than manually cutting and pasting the texts from one transcribed document to another. The NVIVO creates a platform for the researcher to manage the data to answer their research questions. Azeem et al. (2012) indicate, “In short, NVIVO assists in the management and synthesis of ideas” and “offers a variety of analysing tools for developing new understandings and theories about the data and testing of answers to research questions”.

A sample of how we conducted our analysis using the NVIVO software is illustrated below:



Name	Files	References
EFFECTIVENESS	0	0
General	8	25
Improvement	9	33
IS MANAGMENT	0	0
Effectiveness	9	46
Emphasis	9	49
Responsibility	9	52
Snr Management Role	8	27
POLICY	0	0
Awareness	0	0
Devt	1	1
Status	6	11
Content	9	27
Devt Process	1	1
Challenges	9	37
Effectiveness	8	13
Participants	8	25
Senior Mgt Role	8	13
Enforcement	0	0
Compliance Awaren...	6	11
Compliance Enforce...	1	1
Rewards	7	17
Sanctions	8	22
Compliance Monitori...	0	0
General	8	41
Snr Mgt role	8	24
Compliance Status	3	7
Evolution	0	0
Challenges	2	4
Effectivenness	5	7
Participants	7	13
Snr Mgt Role	7	8
Importance	9	26
Status	9	33

Figure 3: Sample of how we conducted our analysis using the NVIVO software

In addition, we used recommended guidelines for thematic analysis as detailed below to identify the themes and sub-themes:

Guidelines for thematic analysis

The concept of thematic analysis is the most common and accessible approach for qualitative data analysis. It is primarily used for identifying patterns of similarity and differences in research data analysis. According to Boyatzis, (1998), it helps a researcher to "minimally organise the data and describe it in a rich detail". The thematic analysis approach also helps in "identifying, analysing, and reporting patterns (themes) within data" (Braun & Clarke, 2006).

In this study, we used the thematic analysis method because it "can produce an insightful analysis that answers particular research questions" (Braun & Clarke, 2006) as well as "providing a rich and informative but complex account of results" (Bamaga et al., 2024). For instance, to clarify the findings better, we used the NVIVO software to code the responses into codes, subthemes, themes, and categories. Zhang and Wildemuth (2016) state that categories are derived from three sources: The data, previous related studies, and theories, and that coding schemes can be developed inductively and deductively. We used a deductive, bottom-up approach for this research to carry out our analysis. The themes and categories were theory-driven and informed by the literature review. In general, such research, as in the case of Qualitative analysis, always has a degree of interpretation. However, the degree of interpretation can be mitigated by providing the coding framework for clarity (Bryman, 2012). In more specific details, we used the NVIVO software as an effective analysis method and the process we used to conduct the thematic analysis is as follows:

- Familiarisation: After completing the interviews, the researcher played the audio and matched them to the transcription by thoroughly reading them. This is to help the researcher to understand and be conversant with the data.
- Code Generation: The researcher developed the initial codes based on the questions and responses received by focusing on the data's key issues (three categories). The codes were the features (themes) the researcher identified during the familiarisation process. As part of this process, the researcher developed visible coding stripes to show the codes used and how their content was coded.

- Themes Generation: We used the nodes to identify broader patterns by collating and categorising the codes. This resulted in the themes. The themes were further grouped under the three main categories.
- Reviewing and Naming Themes: After identifying all themes in the data and organising themes through the iterative process, we categorised themes into meaningful sub-themes to develop a thematic framework under the three categories by putting similar themes and ideas into groups and the thematic framework.

3.11.5 Study Procedures

Before the study, ethics approval was obtained from our department's Ethics Committee for all the studies. We also obtained approval from the NIA and the external stakeholders to engage the staff and management members. All participants in the four studies were over the age of 18 and consented to participate in the study.

3.11.6 Data Quality

Before the survey analyses, the datasets were examined for quality to ensure that only attentive responses and those representative of normal answers were retained. Methods for identifying careless responses (Meade & Craig, 2012) were implemented to filter out participants who may not be paying attention. This was done by following Janssens et al.'s (2008) advice on the use of statistical analysis in helping to sort out data into smaller, meaningful statistical displays. For instance, as a red herring mechanism, we added a question asking participants to write the page number on each page.

For the interview data, we transcribed them from audio into Microsoft Word using the "Temi" software application. Using the application, we played the audio and matched them to the transcribed Microsoft words to ensure that they were the exact statements or words used by the respondents. To facilitate their analyses, we uploaded the Microsoft Word transcriptions into the NVIVO software and each participant was assigned a unique identifier.

We also used the demographic profile of participants, which included Gender, Age range, Department or Unit, Years of work, Educational background, Operational region, and Type of employment to check whether the participants formed a representative sample of the organisation's employee population, by comparing their data to the demographic information from the organisation's Human Resource Data.

3.11.7 Reliability/Scale Validity

Reliability measures the internal consistency of a latent variable, the degree to which several measurement items that reflect it are inter-correlated (Hair et al., 1998; Nunnally and Bernstein, 1994). According to Peterson (1994), Cronbach alpha is the most commonly used measure of reliability in non-structural equation modelling analyses. The Cronbach alpha is considered the de facto measure of scale reliability. Reliability measures the degree to which the measurement items that reflect the same latent variable agree (Campbell and Fiske, 1959; Churchill, 1979). According to Churchill's seminal work, "Coefficient alpha absolutely should be the first measure one calculates to assess the quality of the instrument". When the reliability of a latent variable is low, the standard practice is to drop items until the coefficient reaches the desired threshold (Churchill, 1979). Coefficient alpha measures the average ratio of item variance to scale variance, accounting for the number of items in the scale (Cronbach, 1951). According to Cronbach (1951), a value of 0.6 or above is regarded as a good indicator of internal consistency.

The extent of variability spread or dispersion of our data (the data's spread rate) was also assessed. The mean and standard deviations were used to analyse the central tendency of the data. The Standard Deviation was used to know the range of the data or measure of dispersion for the data. Even though the appropriateness of using the mean and Standard deviation for the Likert scale has been debated, it is generally accepted. According to Jamieson (2004), the arguments about the suitability of using the mean and standard deviation of the Likert scale can be grouped under the following viewpoints:

- That the response categories in Likert scales have a rank order, but the intervals between values cannot be presumed equal.
- That the mean (and standard deviation) is inappropriate for ordinal data
- That treating ordinal scales as interval scales has long been controversial.
- It has become common practice to assume that Likert-type categories constitute interval-level measurement.
- Issues such as levels of measurement and appropriateness of mean, standard deviation, and parametric statistics should be considered in the design stage and addressed by authors.

The views outlined are detailed below:

3.11.7.1 The Response categories in the Likert scales have a rank order, but the intervals between values cannot be presumed equal

Some researchers argue that Likert scales have a rank order, but the intervals between values cannot be presumed equal and should not be used. This position is shared by Cohen et al. (2000), Hansen (2007), and Pett (1997). For instance, according to Cohen L.et al. (2000), "Likert scales are commonly used to measure attitude, providing a range of responses to a given question or statement". According to Pett (1997), Likert scales generally "fall within the ordinal level of measurement". To further explain the above points, Cohen et al. (2000) and Clegg (1998) have indicated that "the legitimacy of assuming an interval scale for Likert type categories is an important issue because the appropriate descriptive and inferential statistics differ for ordinal and interval variables" and if the wrong statistical technique is used, the researcher increases the chance of coming to the wrong conclusion about the significance (or otherwise) of his research" Jamieson (2004).

Although Blaikie (2003) explains that researchers have frequently assumed that the intervals between the values on the Likert scale are presumed to be equal, Cohen et al. (2000), however, contend that "it is illegitimate to infer that the intensity of feeling between "strongly disagree" and "disagree" is equivalent to the intensity of feeling between other consecutive categories on the Likert scale".

3.11.7.2 The mean (and standard deviation) is inappropriate for ordinal data

According to Blaikie (2003) and Clegg (1998), it is appropriate to use the mode or median to measure the central tendency because "the arithmetical manipulations required to calculate the mean (and standard deviation) are inappropriate for ordinal data". Blaikie (2003) further indicates that "ordinal data may be described using frequencies ⁄percentages of response in each category".

3.11.7.3 Treating ordinal scales as interval scales has long been controversial

Some scholars have recently ignored the "rules" on ordinal scales and have treated their data as interval scales despite using a Likert scale and mean and standard deviations. They have even performed parametric analyses such as ANOVA. This is in line with Blaikie's (2003) observation on how common it is to see the assumption where Likert-type categories constitute interval-level measurement by some scholars. Such scholars do not generally make it clear whether they are aware that their action or work would be regarded as illegitimate, neither do they also make statements about an assumption of interval status for Likert data, and no argument is made in support (Jamieson, 2004).

3.11.7.4 It has become common practice to assume that Likert-type categories constitute an interval-level measurement

According to Knapp (1990), how some scholars treat ordinal scales as interval scales has long been controversial. Knapp sees some merit in the argument that sample size and distribution are more important than the level of measurement when determining whether it is appropriate to use parametric statistics. However, he explains that even if one accepts that it is valid to assume interval status for Likert-derived data, the data sets generated with Likert-type scales are mostly skewed or polarised distribution.

3.11.7.5 Such issues as levels of measurement and appropriateness of mean, standard deviation and parametric statistics should be considered in the design stage and must be addressed by the authors

Generally, there is a view that levels of measurement and appropriateness of mean, standard deviation, and parametric statistics should be considered when designing, and they must be addressed in the chosen methodology. This view is held by scholars such as Knapp (1990), who advised that "the researcher should decide what level of measurement is in use" and that "non-parametric tests should be employed if the data is ordinal, and if the researcher is confident that the data can justifiably be classed as interval, attention should nevertheless be paid to the sample size and to whether the distribution is normal".

In this research, we categorised the Likert scale as an interval scale with equal distance between each anchor. This conforms with the Stevens' measurement framework where Likert scale-type items are summed or averaged and presented horizontally (Uebersax,2006). Additionally as noted in Chapter 3, under the Questionnaire Analysis section, Dehaene et al (1990, 1993), Zorzi et al (2002) and Cohen et al,(2011) justify this by highlighting that recent investigations indicate that such an approach helps humans to have a mental representation of numbers that seems to resemble a mental number line" (Spencer et al, 2015).

To provide a more transparent relationship among the variables, we used the concept of correlation coefficient to statistically measure the strength and directions.

3.11.7.6 Correlations

A correlation is a statistical test used to measure the extent of the relationship between two or more variables. The strength and direction of the relationship between the variables are measured as a correlation coefficient. According to Haaker (2019), "correlation coefficients measure the strength of the association between two variables".

A positive correlation indicates that an increase in one variable leads to an increase in the other variable and vice versa. On the other hand, a negative correlation indicates that an increase in one variable leads to a decrease in the other variable and vice versa. The absolute values of the coefficient determine the strength of the correlation as indicated by Schober et. al (2018) are below:

0.0 - 0.2 Very weak

0.2 - 0.4 Weak

0.4 - 0.6 Moderate

0.6 - 0.8 Strong

0.8 - 1.0 Very Strong

Source: Schober et. al (2018)

On the qualitative research aspects, Bjorck (2001) uses a qualitative method to study information security consultants' experiences and insights in implementing and certifying information security management systems (ISMS). Bjorck (2001) used the qualitative method to define critical success factors for implementing and certifying Information Security Management Systems (ISMS). This means that using research methods could enable the researcher to provide a descriptive and detailed analysis of the attitudes, behaviours and characters of people or other research settings. Despite these benefits, "the small selective sample size is related to the in-depth nature of the qualitative approach (Carr, 1994). Cohen et al. (2007) point out that "qualitative data analysis involves organising, accounting for and explaining the data; in short, making sense of data in terms of the participants' definitions of the situation, noting patterns, themes, categories and regularities…the analysis will also be influenced by the number of datasets and people from whom data have been collected". This means that the time for the research work potentially affects the findings of the researcher. Al-wadi (2009) indicates, "Someone else conducting the same qualitative research at a different time could reveal something quite different". Qualitative methods include, for example, interviews, observation and ethnography.

3.12 Concluding Remarks

In this chapter, the researcher justifies the four studies to be conducted using the NIA as a case study and a mixed study approach. The chapter also details vital methodological issues to consider for research of that nature.

The following chapters will focus on the four studies. It will discuss the aims and objectives of the survey, the study design and their methods, participants and procedures, analysis and results, and discussions on the teaching of the studies.

4 Study 1 on Internal Stakeholders Survey (NIA Staff Survey)

This chapter focuses on the quantitative report analysis of the data collected from the junior and middle staff survey. As noted in Chapter 3, this study aims to understand the perception and beliefs of the junior and middle staff and their involvement in the development, enforcement, evolution and compliance with the NIA ISP. It also seeks to determine the extent of employees' awareness and understanding of the NIA ISP. The chapter also discusses the questionnaire designs, data analysis, results, and conclusions from the study. The study broadly examined important considerations for electronic information systems for professionals and academia.

4.1 Study Design

The research objectives for this study are:

- To determine the extent of awareness and understanding of the ISP by NIA staff.
- To assess the perceptions/feelings of the NIA staff about the content and provisions of the ISP.
- To understand ISP compliance from the perspective of the NIA staff.
- To determine the involvement of the staff in the policy formulation, implementation and evolution processes.

To achieve our aim of understanding the awareness, perception/beliefs, involvement and compliance to the NIA ISP, we designed a questionnaire to assess the junior and middle employees' ISP awareness perception; ISP Communication; ISP Readability, Reasonability, Practicality and Comprehension; ISP Rewards; ISP Intrinsic Benefits; Attitudes towards ISP Compliance and real ISP violations in the NIA (see details in Appendixes 9.1, 9.2 and 9.3 for the PIS, ethics and questionnaire). The details for the adapted questions for the non-demographic questions are as presented below:

Theme	**Adopted Author/Source**	**Questions**
ISP Awareness	Bulgurcu et al. 2010 (3 Questions)	I know the rules and regulations prescribed by the Information Security Policy (ISP) of my organisation. I understand the rules and regulations prescribed by the ISP of my organisation.

		I know my responsibilities as prescribed in the ISP to enhance the IS security of my organisation.
ISP Effectiveness	Adele Da Veiga 2018 (5 Questions)	National Identification Authority (NIA) communicates relevant information security requirements to me. The information security policy is practical. I am informed in a timely manner as to how information security changes will affect me. The contents of the information security policy were effectively communicated to me. The contents of the information security policy are easy to understand.
Rewards	Adapted from Bulgurcu et al. 2010 (4 Questions)	My pay raises and/or promotions depend on whether I comply with the requirements of the ISP. I will receive personal mention in oral or written assessment reports if I comply with the requirements of the ISP. I will be given monetary or non-monetary rewards if I comply with the requirements of the ISP. My receiving tangible or intangible rewards are tied to whether I comply with the requirements of the ISP.
Intrinsic Benefits	Adapted from Bulgurcu et al. 2010 (4 Questions)	My compliance with the requirements of the ISP would make me feel content. My compliance with the requirements of the ISP would make me feel satisfied. My compliance with the requirements of the ISP would make me feel accomplished. My compliance with the requirements of the ISP would make me feel fulfilled.
Most common ISP Violations	Adapted from Siponen and Vance 2010 (9 Question)	Failing to lock or log out of workstation constitutes an Information Security Policy violations. Writing down personal passwords in visible places constitutes an Information Security Policy violation. Sharing passwords with colleagues or friends constitutes an Information Security Policy violation.

		Copying sensitive data to unencrypted USB drives constitutes an Information Security Policy violation. Revealing confidential information to outsiders constitutes an Information Security Policy violation. Disabling security configurations constitutes an Information Security Policy violation. Using laptops carelessly outside of the company constitutes an Information Security Policy violation. Sending confidential information unencrypted constitutes an Information Security Policy violation. Creating easy-to guess-passwords constitutes an Information Security Policy violation.
Attitude towards Compliance	Adapted from Bulgurcu et al. 2010 (4 Question)	1a. To me, complying with the requirements of the ISP is Necessary. 1b. To me, complying with the requirements of the ISP is Unnecessary. 2a. To me, complying with the requirements of the ISP is Beneficial. 2b. To me, complying with the requirements of the ISP is unbeneficial. 3a. To me, complying with the requirements of the ISP is important. 3b. To me, complying with the requirements of the ISP is unimportant. 4a. To me, complying with the requirements of the ISP is useful. 4b. To me, complying with the requirements of the ISP is useless.
ISP Readability and Comprehension	Own Questions (4 Questions)	My organisation educates employees on their computer security responsibilities. The ISP of the NIA is reasonable. The ISP of the NIA is not readable. The ISP of the NIA is not easy to understand.
NIA ISP Development and Evolution Process	Own Questions (4 Questions)	In my organisation, ISP development and revision involves all employees. During the development and any revisions of the ISP, employees are consulted to ensure that its provisions are and remain reasonable. During the development and any revisions of the ISP, its phrasing is tested with employees to ensure that it is and remains easy to read.

		During the development and any revisions of the ISP, employees are actively involved in ensuring it is and remains easy to understand.

Table 2 Non-demographic questions and adopted Sources for this study

4.2 Participants and Procedures

Participants and procedures are discussed in the sections below.

4.2.1 Participants

This study involved distributing 150 paper Questionnaires to the NIA's Middle and Junior Staff throughout Ghana's four operational regions. As noted in Chapter 3, participant and study procedure section, we administered the questionnaire to the employees between 14/02/2020 and 20/10/2020. The long length of the data collection was due to the Covid-19 restrictions. Again, we distributed the questionnaire based on a distribution formula primarily based on the actual staff strength of each unit or department in the various operational zones or offices to ensure fair participation from each unit or department.

The focus of this research was on the permanent and contract staff. To this effect, we distributed the 150 questionnaires manually to the contract and permanent staff, and 115 were returned to us. This represents 76.7% of total participation.

Out of the 115, three questionnaires were excluded because they were incomplete. We manually collected the results of the self-administered questionnaire, which were later entered into Qualtrics for ease of analysis. The manual data collection ensured easy access to participants and was due to the unstable internet connectivity in the regions we collected the data from.

4.2.2 Study Procedures

This study focused on assessing the extent of awareness, understanding, involvement and compliance of Junior and Middle staff of NIA to their ISP, so we designed a questionnaire with adopted questions from authors and adopted the 7-point Likert scale. Regarding the demographic questions for the junior and middle staff, the questionnaire covered seven (7) demographic questions that included Gender, Age range, Education, Employment type, Years spent at NIA, Department/Unit and NIA Location

4.3 Analysis

As noted in the study design section in Chapter 3, we distributed 150 manual questionnaires and received 115 responses. Out of the 115, three questionnaires were excluded because they were incomplete. We also used methods for identifying careless responses (Meade & Craig, 2012) to filter out participants who may not have been paying attention. We used red herring questions and participants' response times to identify the careless responses.

After that, we first entered the data responses from the paper questionnaires into Qualtrics. We then reviewed and verified all responses, and imported, and stored the data into the Statistical Package for Social Science (SPSS) software to sort the data into smaller units, as recommended by Janssens et al. (2008). Each participant was assigned a unique identifier. We then grouped each participant's data into Demographic and Non-Demographic Data for further analysis.

4.4 Results

The results are discussed under two main sections: demographic and non-demographic results.

4.4.1 Demographic

Under the demographic results, we analysed respondents' data such as their gender, age, department or unit, years of work, employment type, operational region and level of education. We did further analysis by combining some of these demographics and comparing them to the data from the NIA Human Resource (HR) department. The essence of doing this is to know if the research data reflects the reality in the organisation and to check the quality of the data collected.

Table 2 provides an overview of the participants' demographic data (see column Participant Data) compared with data from the Human Resources department of the NIA (see column Organisation Reality).

Category	**Subcategory**	**Participant Data**	**Organisation Reality**
Gender	Male	54% (60)	74.0% (172)
	Female	46% (52)	26.0% (61)

Age Range	20-30	51.8% (58)	44.9% (96)
	31-40	38.4% (43)	45.8% (98)
	41-50	8.0% (9)	7.0% (15)
	51-60	1.8% (2)	2.3% (5)
Department or Unit	Human Resources	8.0% (5)	2.0% (9)
	Administration	6.3% (7)	52.0% (112)
	Technology and Biometrics	41. 1% (47)	22.0% (48)
	Operations	31.3% (24)	11.0% (35)
	Finance	3.6% (4)	6.0% (12)
	Internal Control	2.7% (3)	1.0% (3)
	Other	2.7% (3)	3.0% (6)
	Procurement	4.5% (5)	2.0 (5)
Years of Work	Less than 1year	55.4% (62)	32.0% (68)
	1-2years	12.5% (14)	4.2% (9)
	3-9years	4.5% (5)	3.3% (7)
	More than 9years	27.7% (41)	60.7% (130)
Employment Type	Permanent	30.4% (34)	64.0% (137)
	Contract	65.2% (70)	33.0% (73)
	Seconded	4.5% (5)	3.3% (7)

Table 3: Overview of Study Demographic Data

Table 2 shows a male dominance of 54% males versus 46% females in total responses. This primarily reflects the actual situation in the NIA, where staff are predominantly males. The NIA has 172 males (117 permanent staff and 55 contract staff) and 61 Females (39 permanent staff and 22 contact staff). It is, therefore, clear that the reality is much more strongly biased against females.

In terms of age distribution, the data indicates that 51.8% were aged between 20-30, representing 58 respondents; 38.4% were aged between 31-40, representing 43 respondents; 8.0% were aged between 41-50, representing nine respondents, and 1.8% were between 51-60 years of age representing two respondents. These findings show that most of the respondents working with the NIA are young. This reflects the situation in the organisation. The NIA is a young public organisation formed in 2003, hence the need to employ new and young staff. The old staff were those seconded to the NIA from other governmental organisations during the formative stages. They were later permanently transferred to NIA.

On departmental distribution, 41.1% of the respondents were from the Technology and Biometrics Department, 31.3% from the Operations Department, 8% from the Human Resources Department, 6.3% from the Administration Department, 4.5% from Procurement, 3.6% from the Finance department, and 2.7% each for internal Control and others. The "others" category includes respondents from units/departments such as Research, Policy Planning, Monitoring and Evaluation (PPME).

Essentially, the above represents the composition of the departments in the NIA. The Administration Department is the only one under-represented due to the unavailability of the drivers. It was due to the ongoing mass registration exercise. The drivers were 97 in total.

On the years of work, 55.4% of the respondents had worked in the organisation for less than a year. 12.5% had worked for 1-2 years, with 4.5% having worked for 3-9 years and 27.7% of the respondents working for more than nine years. For further analysis, the NIA staff were divided into two groups: Experienced staff and inexperienced staff. The experienced staff had spent more than three years working with the NIA. On the other hand, inexperienced staff were grouped as those who have spent less than three years working in the NIA.

Regarding the types of employment, seventy-three of the respondents were contract staff (65.2%), Thirty-four (30.4%) were permanent staff, and Five (4.5%) were seconded staff. Generally, this is what is in practice at the National Identification Authority. A lot more staff are recruited for any mass registration exercise in addition to the regular staff of permanent and contract staff. The NIA has 147 permanent staff members, with 77 contract staff members regularly working for the organisation's day-to-day functions. However, when there is a mass registration exercise, a proportion of the permanent and contract staff (regular ones) are assigned to supervise the field officers who are recruited mainly as new contract/temporary staff. For instance, as part of the previous mass registration, new employees were recruited as data verification and authentication officers on a contract basis. This explains why there are many more contract staff in terms of respondents than their permanent counterparts. Seconded staff are externally sourced or posted to the organisation from other government Ministries, Departments or Agencies (MDAs).

4.4.2 Further Demographic Analysis

To clarify the demographics above, we asked respondents about their educational background and their regions of operations. We believe these questions would enable us to assess whether or not the individual's educational background relates to gender. Regarding the operational regions and departments of respondents, we wanted to match the responses to the actual situation in the organisation to know how decentralised it is. In addition, we assessed the gender versus education of the respondents to know the ratio of male versus female undergraduates and postgraduates. We also assessed the respondents in terms of experience versus inexperienced employees. The details are as follows:

4.4.2.1 Level of Education for Respondents

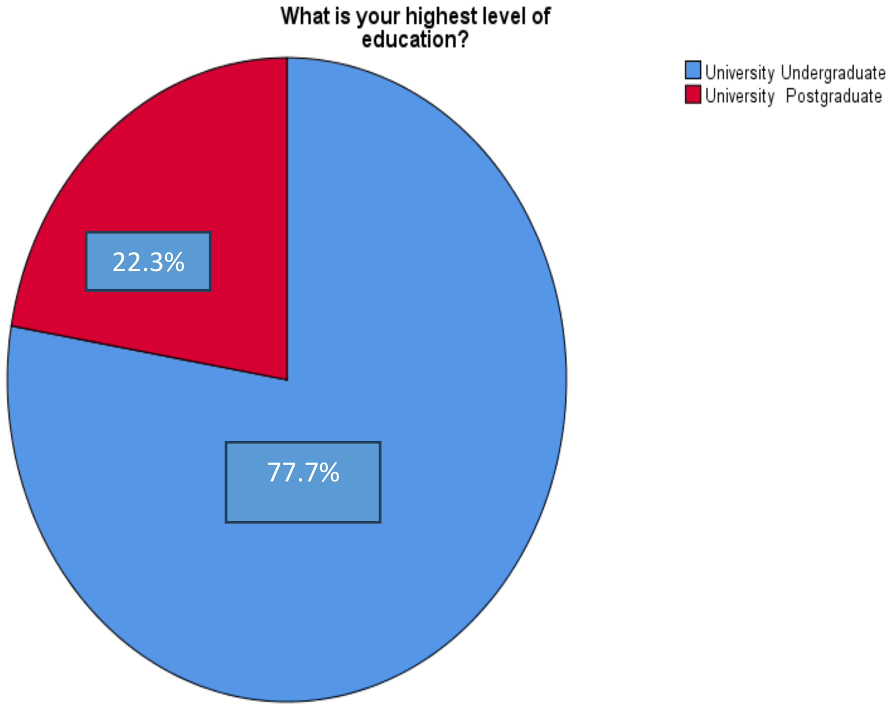


Figure 4: Level of Education of Respondents

From Figure 4, most of the study's respondents noted they had a university undergraduate education. They were eighty-seven in number, constituting 77.7%, while Twenty- five (22.3%) of the respondents noted that they had had a University postgraduate level of education. This is true because the minimum requirement for an employment opportunity for the formal category in the organisation is a first degree. The only exception for this is the driving role and other auxiliary staff.

4.4.2.2 Operational Regions of Respondents

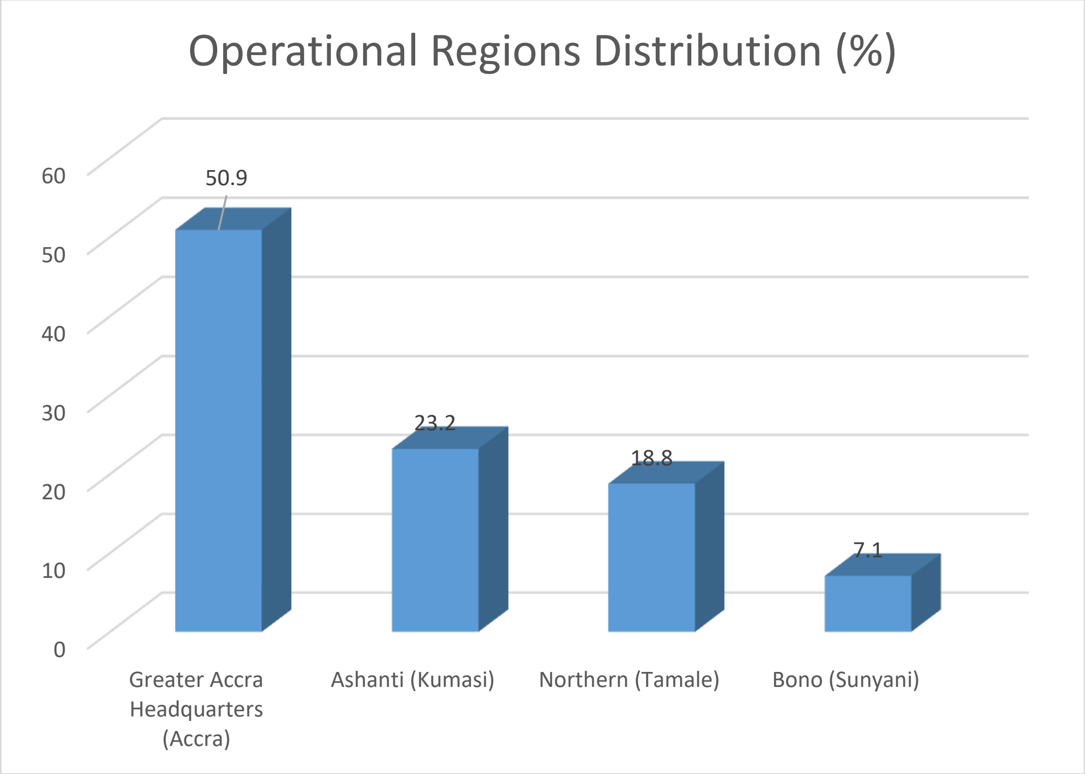


Figure 5: Operational Regions of Respondents

Figure 5 shows that most respondents who participated in the exercise indicated they were in the Greater Accra Headquarters (Accra). They were fifty-seven in number, constituting a percentage of 50.9%. Twenty-six respondents (23.2%) noted that they were from the Ashanti region (Kumasi). Another twenty-one respondents (18.8%) also noted that they were from the Northern region (Tamale). Eight (7.1%) respondents indicated they were from the Bono region (Sunyani).

This reflects the actual situation in the organisation, as most administrative and operational functions are centralised and controlled at the head office. The organisation has yet to fully decentralise and operationalise its functions to the various regions in the country. The NIA has 26 staff in the Ashanti region, which serves as the second largest administrative region, with the Northern region (Tamale) having 21 staff and the Bono region having eight stationed staff. These four offices serve as the operational zonal offices for the nationwide registration exercise throughout the country, which has 16 regions.

4.4.2.3 Responses by Gender and Educational Qualification

The graph below shows that respondents for the main study were post-secondary education and postgraduate education workers at the National Identification Authority (NIA) in Ghana:

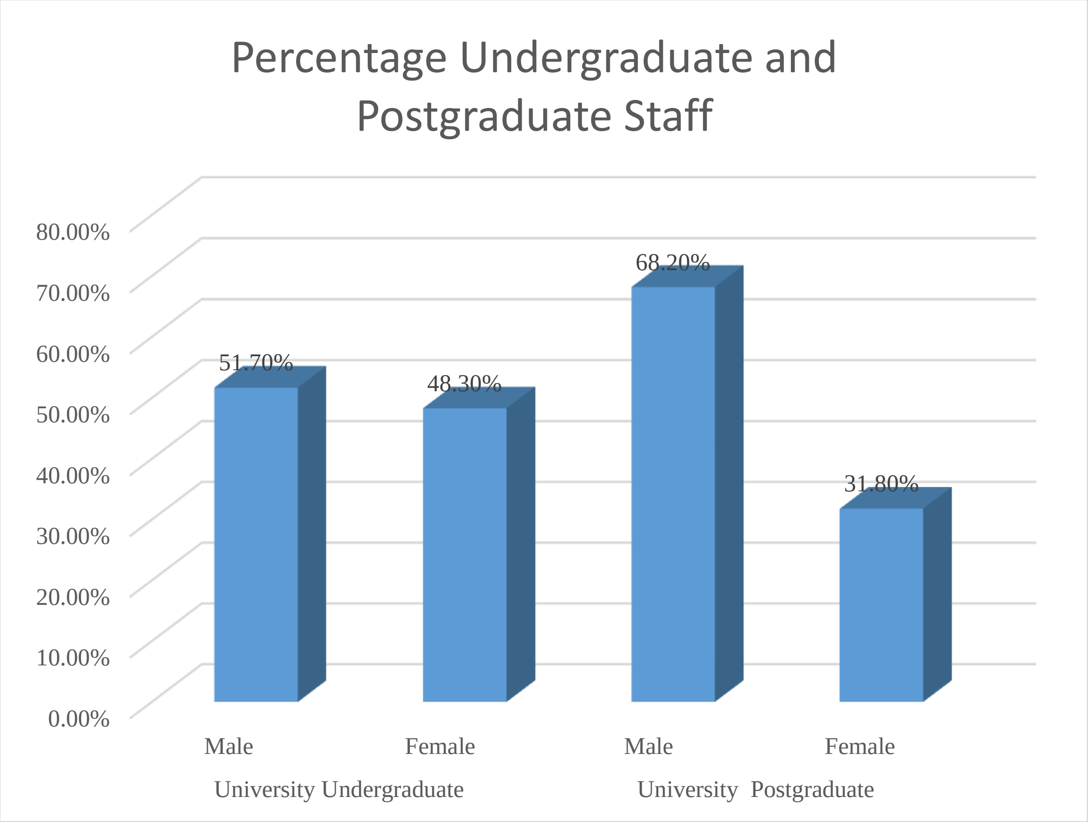


Figure 6: Gender and Educational Qualification of Respondents

From Figure 6, the data effectively shows a male-to-female percentage ratio of 51.7% of Males to 48.3% of females. In straightforward terms, the organisation has many more male university undergraduates than their female counterparts.

Regarding the University Postgraduate staff in the organisation, the data shows a ratio distribution of 68.2% for males and 31.8% for females. This means more male postgraduates than female colleagues with the same educational qualification.

4.4.2.4 Responses by Experience/inexperience

This is detailed below:

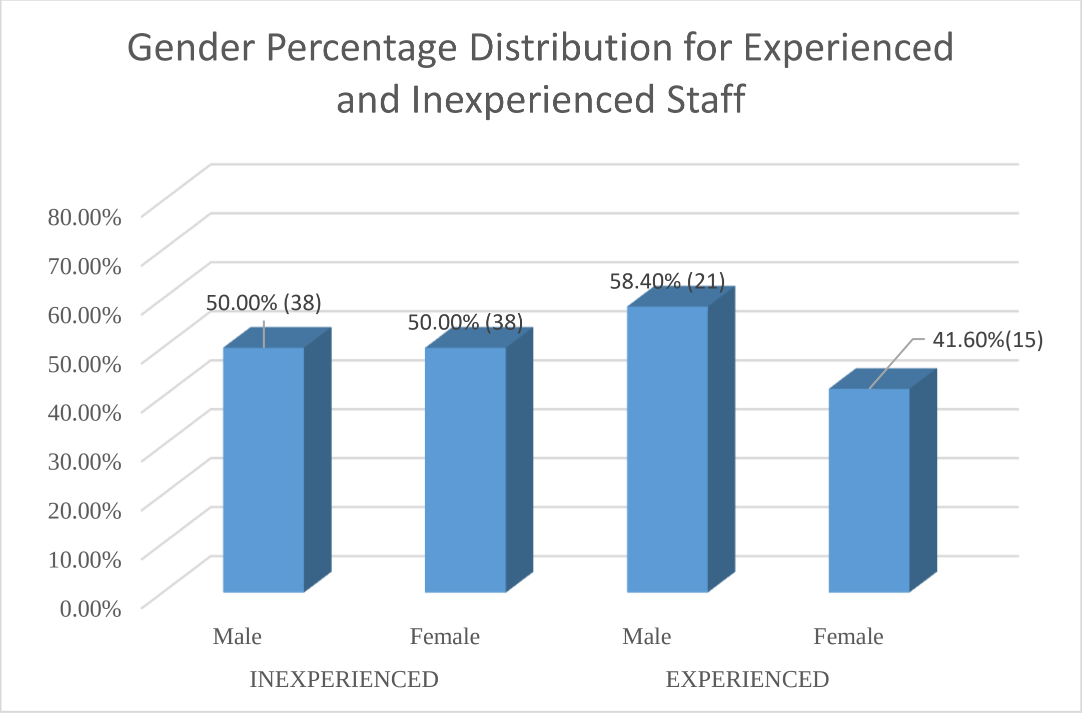


Figure 7: Responses by Gender and Experience/inexperience Distribution

The Figure 7 graph indicates many staff who have been with the organisation for less than a year. This is due to the new mass registration exercise that is currently going on throughout the country. On the other hand, many have worked for the organisation for more than nine years. This category of people includes those who were recruited primarily during an earlier mass registration exercise. This reflects the recruitment strategy of the organisation where they recruits primarily for mass registration or for identity card issuance.

4.4.3 Non-Demographic

On the non-demographic questions, we examine the reliability of the scale used for the questions. The analysis of the questions were done in groups in the following order:

- ISP Awareness
- ISP Communication
- ISP Readability, Reasonability, Practicality And Comprehension
- Extrinsic Rewards For ISP Compliance
- ISP Intrinsic Benefits
- Attitude towards ISP Compliance
- Most Common ISP Violations

4.4.4 Reliability

As noted in Chapter 3, we evaluated the scale's reliability using the Cronbach alpha under the study procedure. We evaluated the ISP Questions under the seven main themes or groups for their consistency, and the results are as presented below:

Summary of the Cronbach Alpha

Item	Cronbach's Alpha	Cronbach's Alpha Based on Standardised Items	No. of Items
ISP Awareness	0.915	0.915	3
ISP Communication	0.909	0.909	4
ISP Readability, Reasonability, Practicality and Comprehension	0.748	0.748	5
Extrinsic Rewards	0.893	0.893	4
ISP Intrinsic Benefits	0.875	0.878	4
Attitude towards ISP Compliance	0.654	0.654	4
Most Common ISP Violations	0.876	0.882	9

Table 4: Cronbach Alpha summary for ISP categories

The Table 3 highlights that the Cronbach alpha for each domain was more than 0.6. This shows that the measures have acceptable reliability, so all were included in the analysis. All the constructs recorded a Cronbach alpha of above 0.8 except for ISP Readability, Reasonability, Practicality and Comprehension and ISP Attitude towards Compliance, which recorded 0.748 and 0.654 respectively. Therefore, none of the items was removed from further analysis.

4.4.4.1 ISP Awareness

The figure 7 below shows how participant responses were distributed for the three (3) ISP awareness questions. Most respondents agreed with the question posed and acknowledged that they know (86%) and understand (80%) the provisions of the NIA ISP. They also indicated they know their responsibilities as prescribed in the NIA ISP (84%). However, some staff were in disagreement with the majority of the respondents. 9% of the respondents disagreed on the ISP knowledge, 12% disagreed on the ISP understanding, and 10% disagreed on their responsibilities. Other respondents were unsure about their position on the question. Those who were unsure were (5% for ISP knowledge, 7% for ISP understanding and 7% for ISP responsibilities).

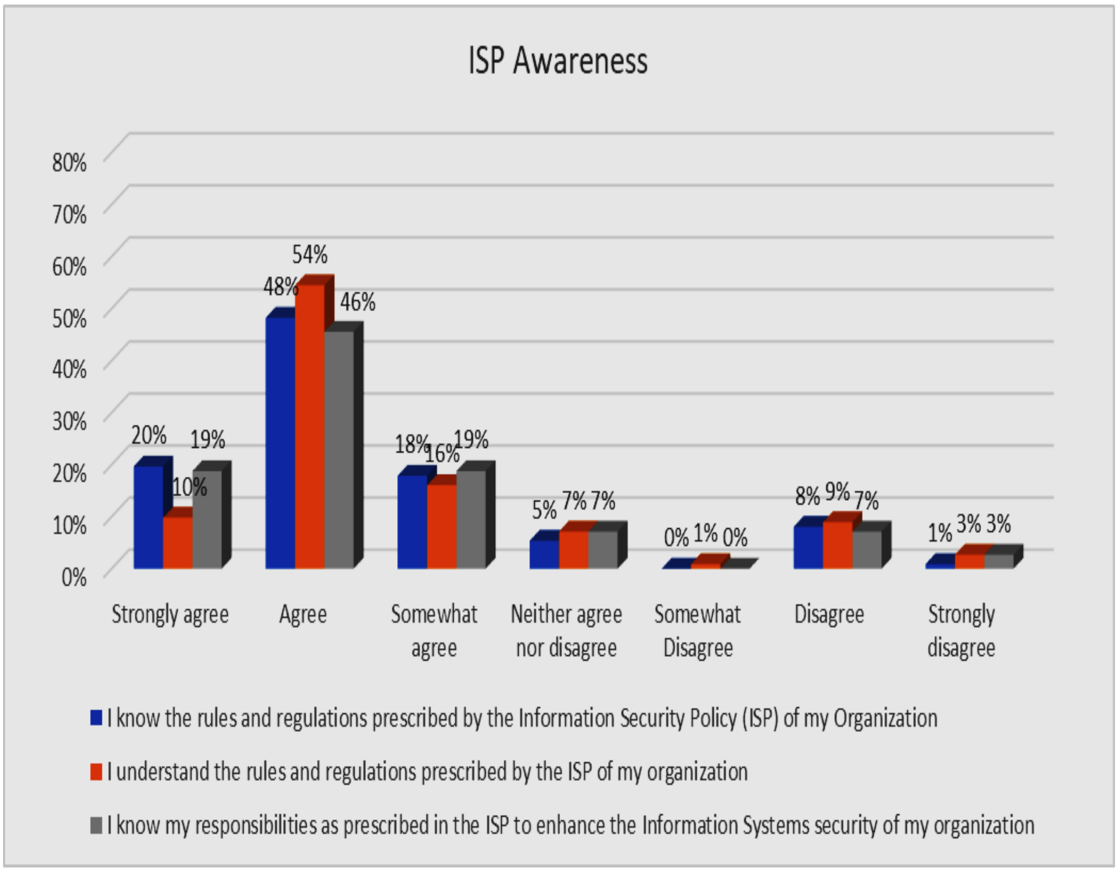


Figure 8: ISP Awareness Distribution

4.4.4.2 ISP Communication

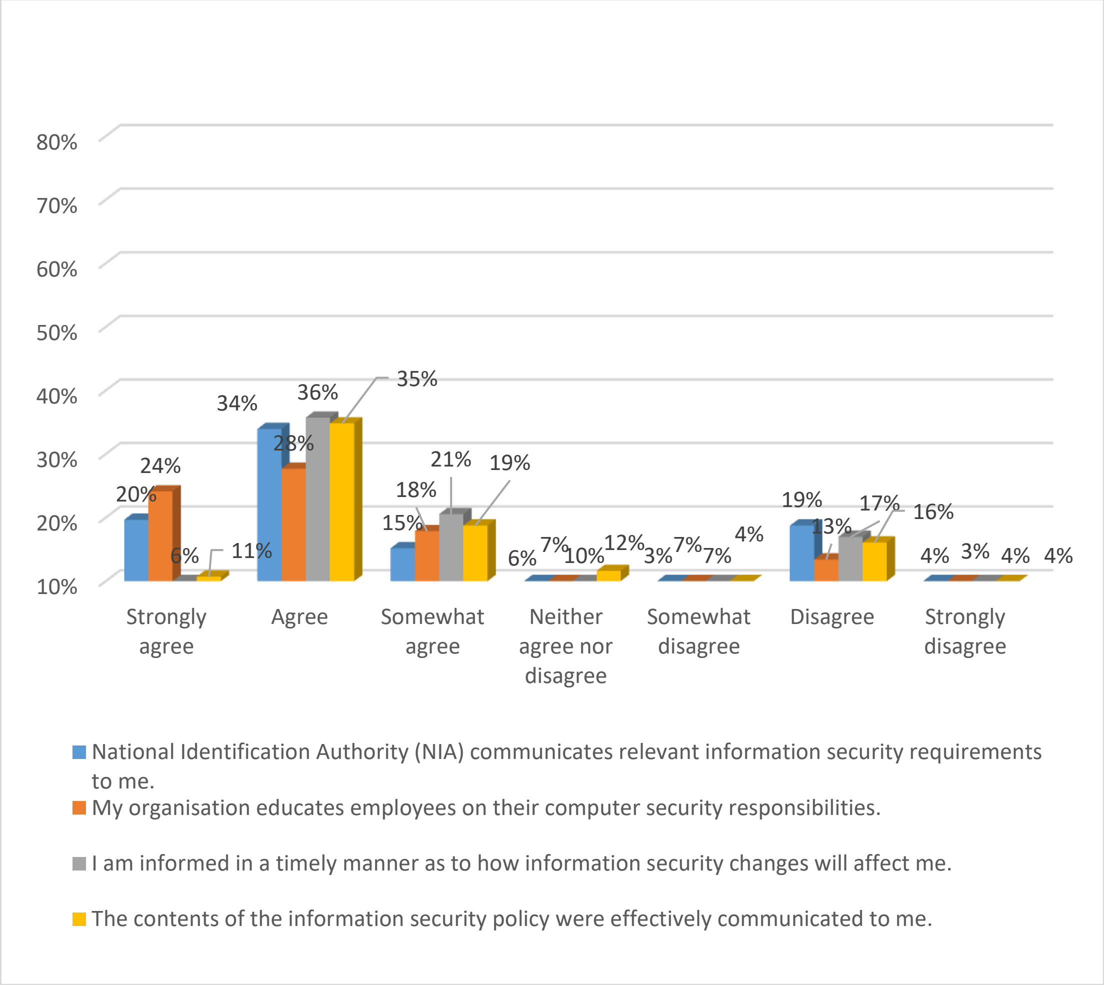


Figure 9: ISP communication Distribution

From the figure 9 above, the majority of the respondents agreed that the NIA communicates relevant information security requirements to them (68%), educates the employees on their computer security responsibilities (70%), inform them on how information security changes affect them in a timely manner (63%) and communicate the contents of the ISP effectively to them (64%). However, 26%, 23%, 27% and 24% respectively disagreed with that assertion, while 6%, 7%, 10% and 12% respectively were unsure about their responses.

4.4.4.3 ISP Readability, Reasonability, Practicality and Comprehension

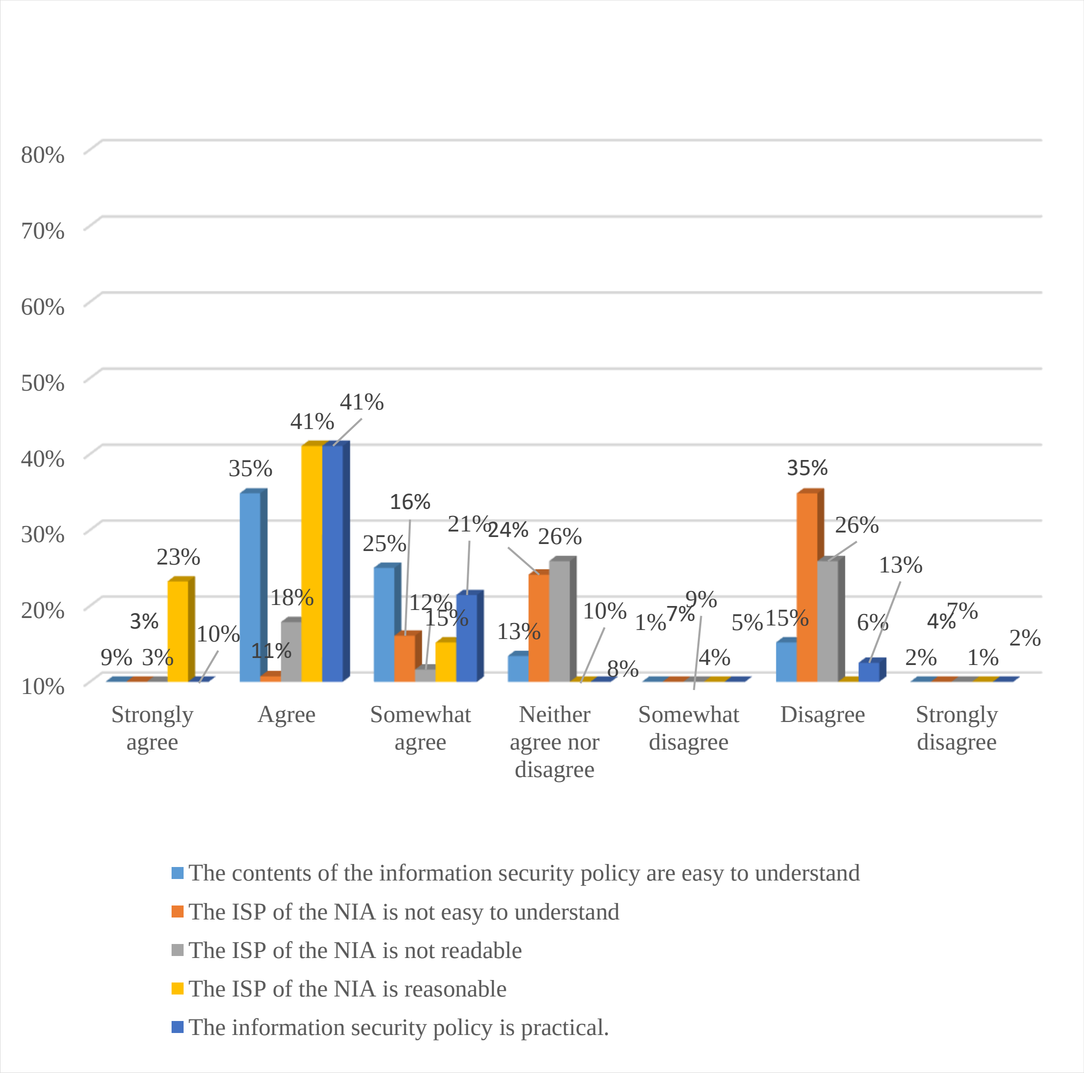


Figure 10:ISP Readability, Reasonability, Practicality and Comprehension Distribution

Figure 10 shows participants' views on the NIA ISP content understanding, ISP non-easiness to understanding, ISP not readable, ISP reasonableness, and ISP practicality. The responses indicate that, for the ISP contents' understanding, 69% agreed cumulatively to it as being easy to understand. However, 18% disagreed cumulatively with that assertion, while 13% of the respondents were unsure about their response.

For the ISP of the NIA not being easy to understand, 30% of the respondents agreed cumulatively to that, while 46% disagreed. Interestingly, 24% also were undecided cumulatively about their response.

On the NIA ISP not readable, most respondents cumulatively disagreed (42%), while 33% cumulatively agreed. 25% of the respondents were undecided on whether they agreed or disagreed cumulatively.

Most respondents cumulatively agreed to the reasonability of the NIA ISP (79%), while 11% disagreed with the majority's position. 10% of the respondents were also unsure about their position.

Cumulatively, 72% agreed that the ISP was practical. However, 20% of the respondents disagreed that it is practical, while 8% of the respondents were unsure.

4.4.4.4 Extrinsic Rewards for ISP Compliance

The figure 11 below shows the participants' perceived extrinsic reward distribution on ISP compliance. The data indicates that most respondents cumulatively disagree that their ISP compliance will be rewarded in monetary/non-monetary (57%) terms. The respondents also disagreed that their ISP compliance would amount to tangible/non-tangible rewards (51%). Only 29% and 32% agree to receive monetary/non-monetary and tangible/non-tangible rewards, respectively. 17% and 14% neither agree nor disagree with receiving monetary/non-monetary and tangible/non-tangible rewards, respectively.

In addition to the above, more participants disagreed that their compliance with the NIA ISP would be rewarded with a pay rise/promotion (46%). However, 35% of the respondents agreed that they would be rewarded with a pay rise/promotion if they complied with their ISP, while 19% neither agreed nor disagreed with that assertion.

In the case of the personal mention/written assessment report question, more participants agreed that their compliance would be rewarded with a personal mention/written assessment report (43%). Despite this, 38% of the respondents disagreed, while 19% neither agreed nor disagreed that they would be rewarded with a personal mention/written assessment report when they comply with the NIA ISP.

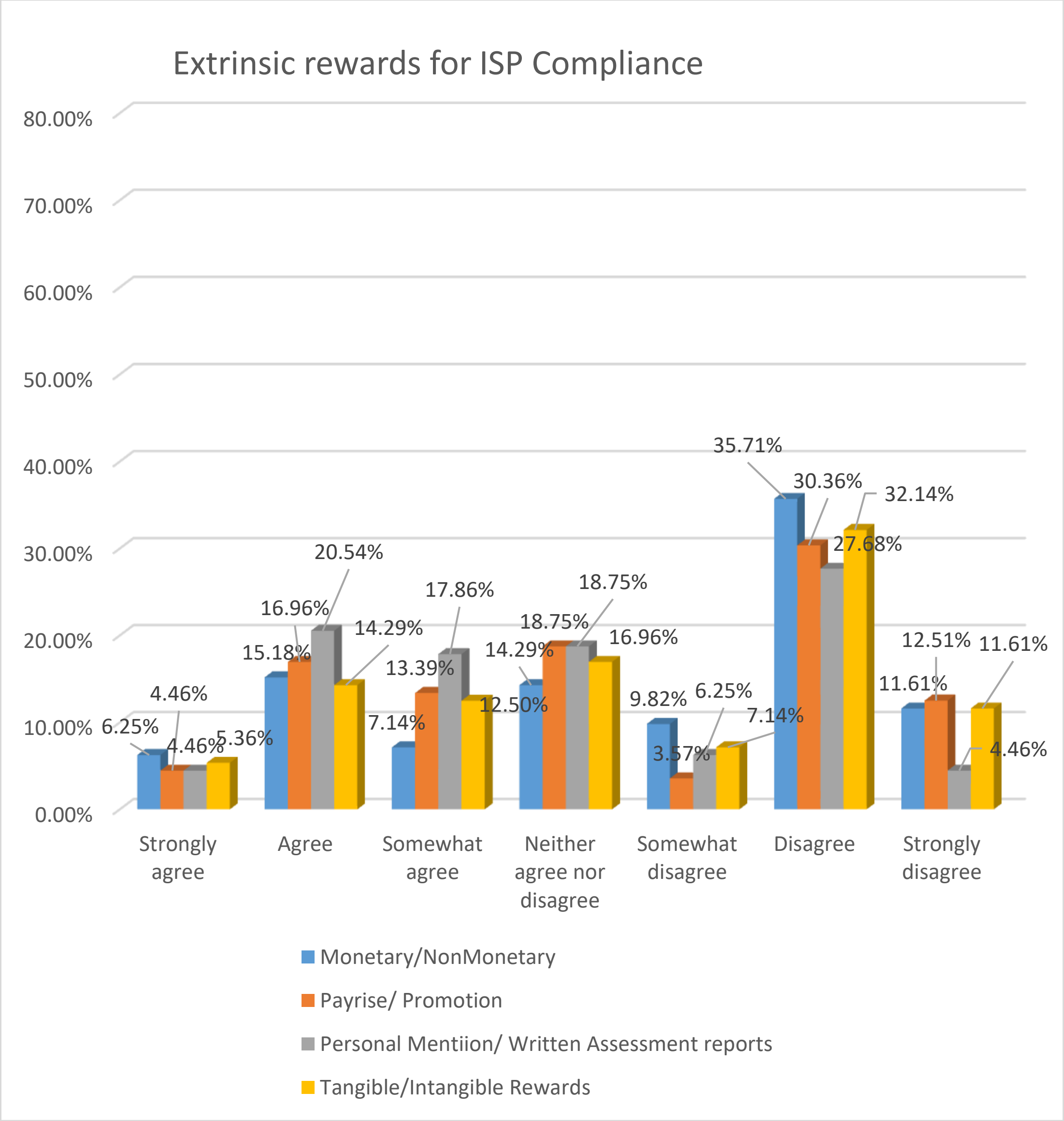


Figure 11: Extrinsic rewards for ISP compliance Distribution

4.4.4.5 ISP Intrinsic Benefits

The distribution of participants' responses regarding their perceived intrinsic benefits of ISP compliance, as shown below, indicates that most staff generally agree that they feel content (68%), feel satisfied (73%), feel accomplished (70%), and feel fulfilled (69%). In addition, 19%, 13%, 20%, and 16% disagreed, and 13%, 14%, 11%, and 15% neither agreed nor disagreed with the questions.

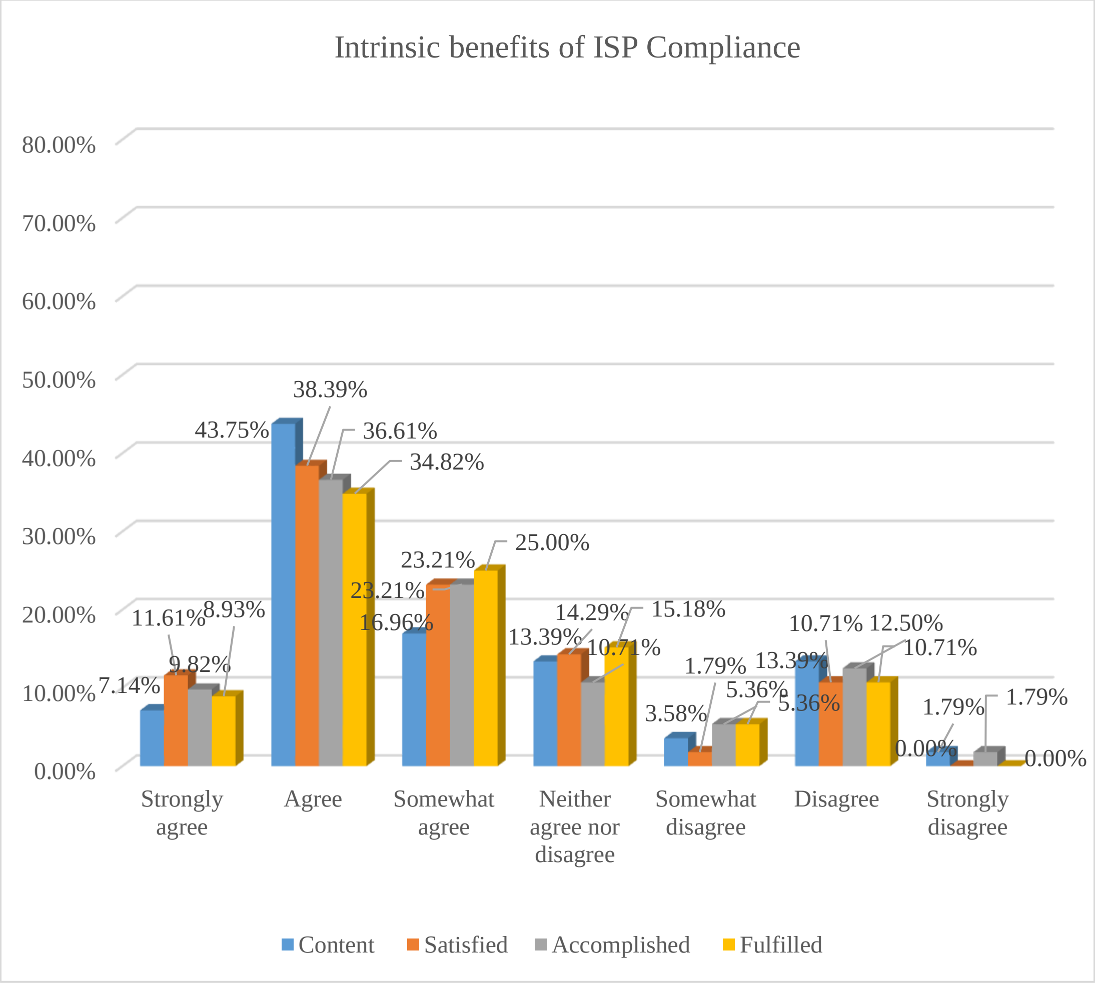


Figure 12:Intrinsic benefits of ISP compliance Distribution

4.4.4.6 Attitude towards ISP Compliance

The figure 13 below shows the distribution of the participants' responses for their attitude towards ISP compliance. Cumulatively, 79% agreed with ISP compliance being necessary, 79% agreed with ISP compliance being beneficial, and 85% agreed with ISP compliance being important, and 87% agreed that the ISP is useful. Meanwhile, 17%, 16%, 10% and 13% disagreed, respectively, and 4%, 5%, 5% and 0% neither agreed nor disagreed with ISP compliance being necessary, beneficial, important and useful, respectively.

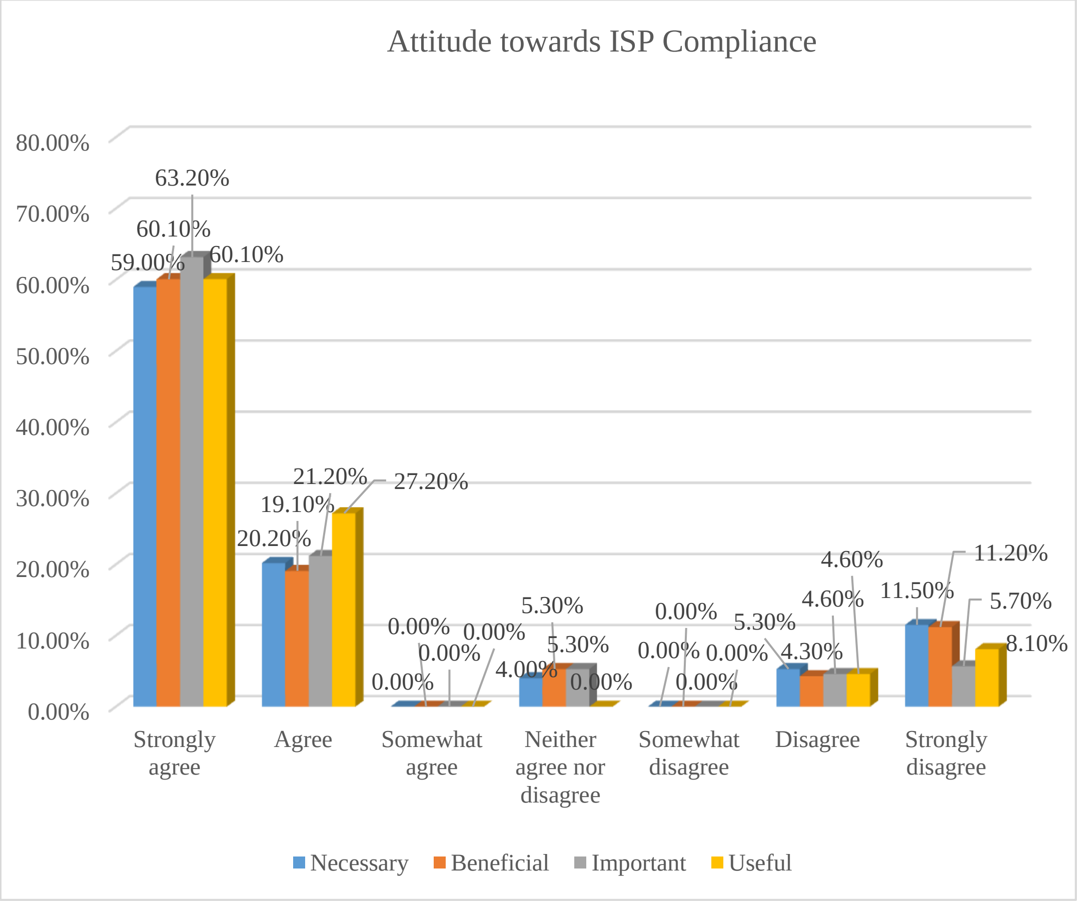


Figure 13:Attitude towards ISP Compliance Distribution

4.4.4.7 Most Common ISP Violations

On the most common ISP violation questions, we grouped questions into three thematic areas. Figure 14 shows information transfer-related violations, figure 15 shows password-related ones, and figure 16 shows workstation-related ones.

Most participants agreed that the questions posed constitute NIA ISP violations in all cases. In terms of levels of agreement on information transfer-related violations, 95% agreed that revealing confidential information to outsiders constitutes an ISP violation, 92% agreed that copying sensitive data to unencrypted USB drives constitutes an ISP violation, and 84% agreed that sending confidential information unencrypted constitute an ISP violation. Regarding disagreement, some participants disagreed (1%, 4%, and 8%, respectively) on information transfer-related violations. Other participants are unsure; they were 4%, 4%, and 8%, respectively, for information transfer-related violations.

On the password-related violations, 84% agreed that creating easy-to-guess passwords constitutes an ISP violation, 89% agreed that sharing passwords with colleagues or friends constitutes an ISP violation, and 91% agreed that writing down personal passwords in visible places constitutes an ISP violation. However, 8%, 2%, and 5% disagreed on password-related violations. Other participants were unsure (8%, 9%, and 5%, respectively) about password-related violations.

On workstation-related violations, 88% agreed that failing to lock or log out of workstations constitutes an ISP violation, with 90% agreeing that using laptops carelessly outside the company constitutes an ISP violation. 91% agreed that disabling security configurations constitute an ISP violation. However, 5%, 6%, and 4% disagreed with workstation-related violations. 7%, 4%, and 6%, respectively, are unsure about workstation-related violations.

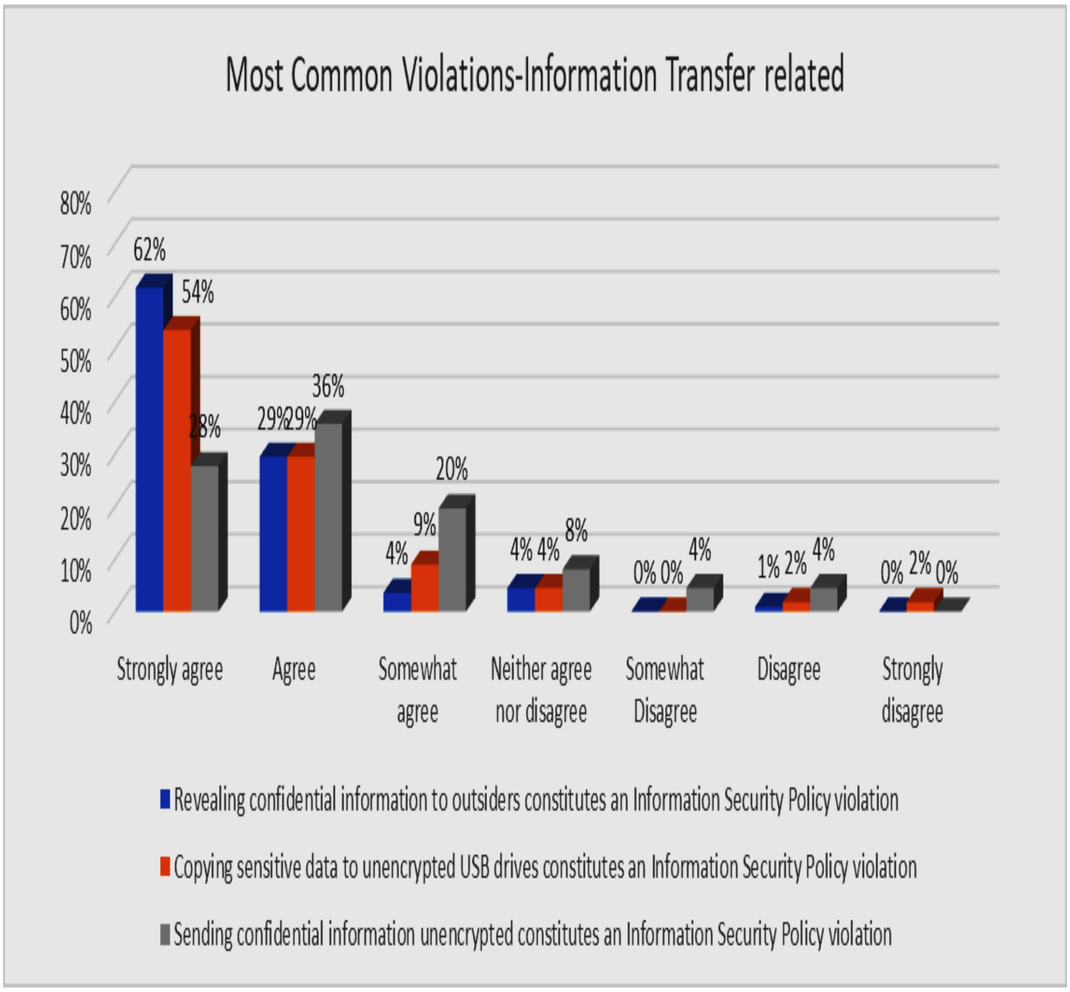


Figure 14: Most Common Information Transfer-related ISP Violations

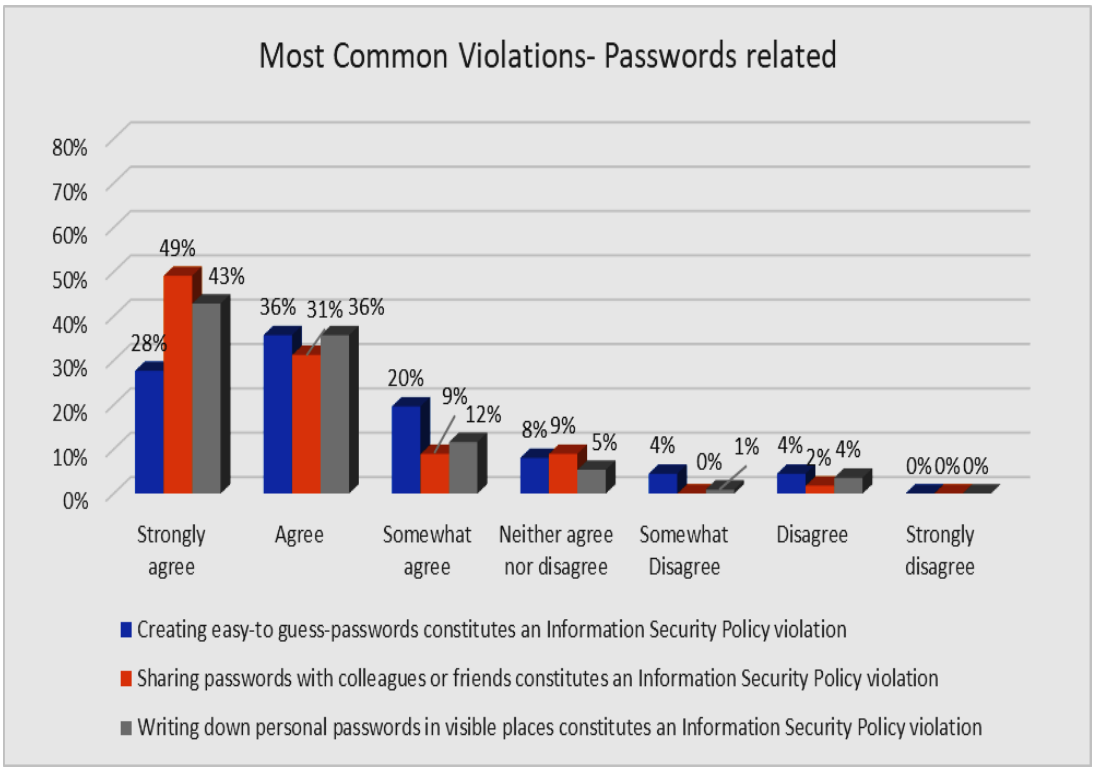


Figure 15: Most Common Passwords-related ISP violations

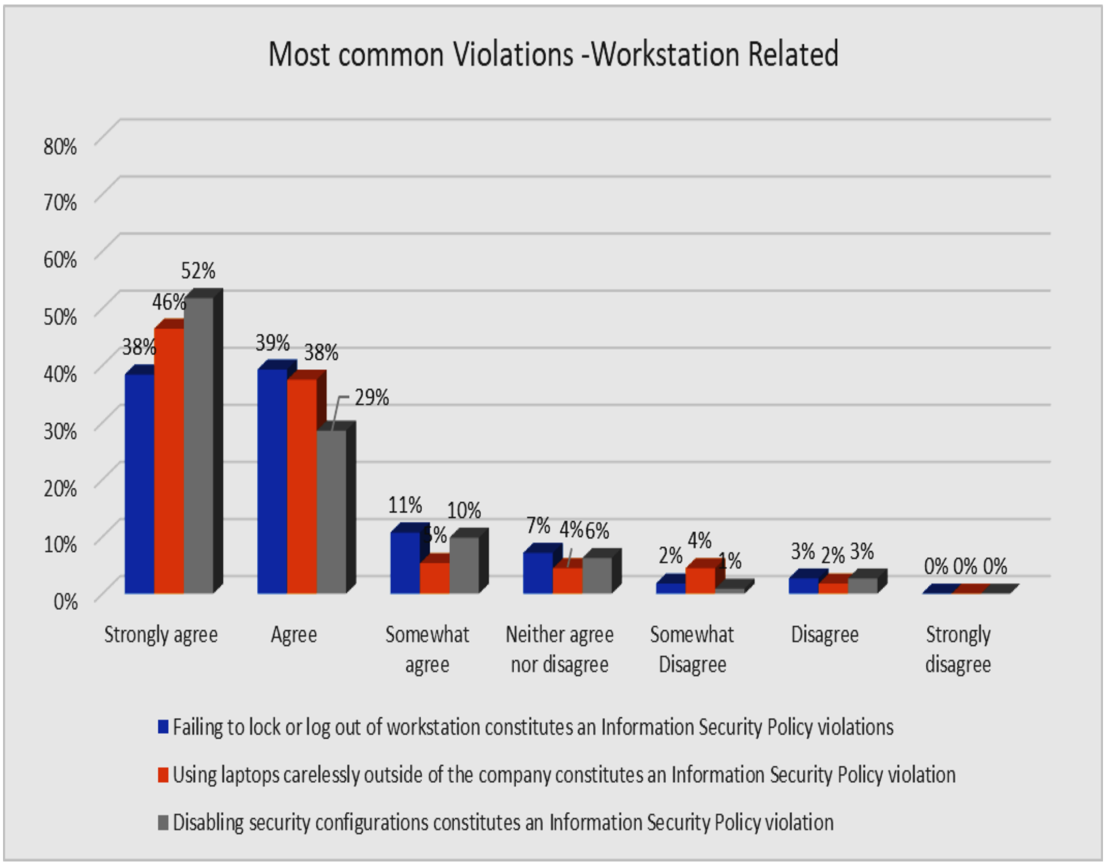


Figure 16: Most Common Workstation-related ISP Violations

4.4.4.8 FURTHER ANALYSIS

ISP Awareness vs Gender and Years of Work

We looked more closely at those who disagreed to establish common characteristics by evaluating their gender, experience (considering those working for the NIA for three or more years as experienced and those less than three years as inexperienced), and department or unit. As we can see in Table 4 below, more female than male participants disagree, with a mix of experienced and inexperienced employees. These participants were also from a range of different departments and units. From the evaluation, we could not establish any clear pattern in the characteristics of these participants that could explain their responses.

ISP Knowledge		
Gender	Experience	Count
Male	Experienced	1
Female	Experienced	4
	Inexperienced	4
ISP Understanding		
Gender	Experience	Count
Male	Inexperienced	2
Female	Experience	4
	Inexperienced	4
Knowledge of Responsibilities		
Gender	Experience	Count
Male	Experienced	1
	Inexperienced	1
Female	Experienced	4
	Inexperienced	2

Table 5: ISP Awareness Characteristics of Disagreeing Participants

ISP Awareness vs Most Common Violations

For further analysis on the ISP Awareness and the most common violations, we opted to use the Mean and the Standard Deviation to analyse the central tendency of the data. The Standard Deviation was used to know the range of the data or measure of dispersion for the data despite the debate about the appropriateness of using the mean and Standard deviation for the Likert scale. This is generally accepted and is in conformity to Stevens' measurement framework where Likert scale type items are summed or averaged and presented horizontally (Uebersax, 2006).

The table below therefore, shows the relationship that exists between ISP awareness and the most common Violation Questions:

Question	**Mean**	**Std. Deviation**
I know the rules and regulations prescribed by my organisation's Information Security Policy (ISP).	2.46	1.381
I understand the rules and regulations prescribed by the ISP of my organisation	2.72	1.490
I know my responsibilities as prescribed in the ISP to enhance the Information Systems security of my organisation.	2.56	1.475
Failing to lock or log out of workstation constitutes an Information Security Policy violation	2.03	1.174
Writing down personal passwords in visible places constitutes an Information Security Policy violation	1.96	1.193
Sharing passwords with colleagues or friends constitutes an Information Security Policy violation	1.85	1.100
Copying sensitive data to unencrypted USB drives constitutes an Information Security Policy violation	1.80	1.229
Revealing confidential information to outsiders constitutes an Information Security Policy violation	1.54	0.879
Disabling security configurations constitutes an Information Security Policy violation	1.84	1.167
Using laptops carelessly outside of the company constitutes an Information Security Policy violation	2.21	1.537
Sending confidential information unencrypted constitutes an Information Security Policy violation	1.88	1.176
Creating easy-to guess-passwords constitutes an Information Security Policy violation	2.39	1.331

Table 6: Means and Standard Deviation of all information security relations

ISP Communication vs Gender, Years of Work, Department and Employment type

On ISP communication, we further analysed the “disagree category” on “The contents of the information security policy are easy to understand” and it revealed that the majority of staff that disagreed on it were permanent staff and were from the Operations and Technology and Biometrics department as below:

Gender	Department	Years of Work	Employment Type
Female	Operations	3-6years	Contract
Female	Operations	More than 9years	Permanent
Female	Operations	More than 9years	Permanent
Female	Technology	More than 9years	Permanent
Female	Technology	Less than 1year	Contract
Male	Operations	More than 9years	Permanent
Male	Administration	More than 9years	Permanent
Male	Finance	6-9years	Permanent
Female	Technology	Less than 1year	Contract
Female	Human Resources	More than 9years	Permanent
Female	Operations	Less than 1year	Contract
Female	Technology	Less than 1year	Contract
Male	Technology	More than 9years	Permanent
Female	Technology	1-2years	Contract
Female	Operations	Less than 1year	Contract
Male	Operations	More than 9years	Permanent
Male	Operations	More than 9years	Permanent

Male	Technology	More than 9years	Permanent
Male	Operations	More than 9years	Permanent
Male	Technology	Less than 1year	Seconded

Table 7: Distribution for general disagreement category on "The contents of the ISP are easy to understand responses"

Further to the above, we noted that a sizeable number of both experienced and inexperienced staff remained neutral on this question, as indicated below:

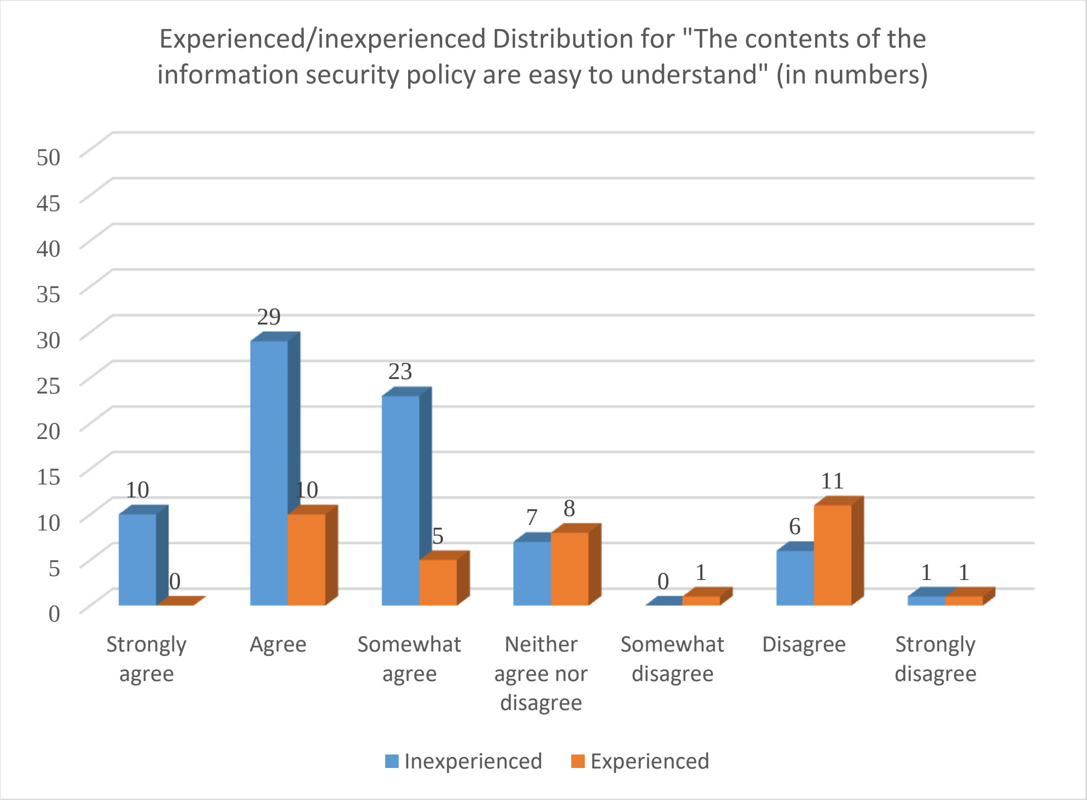


Figure 17: Graphical representation of years of work and "The contents of the ISP are easy to understand"

However, on the "The ISP of the NIA is not easy to understand" question, most of those who remained neutral were new staff. This is illustrated by the table below:

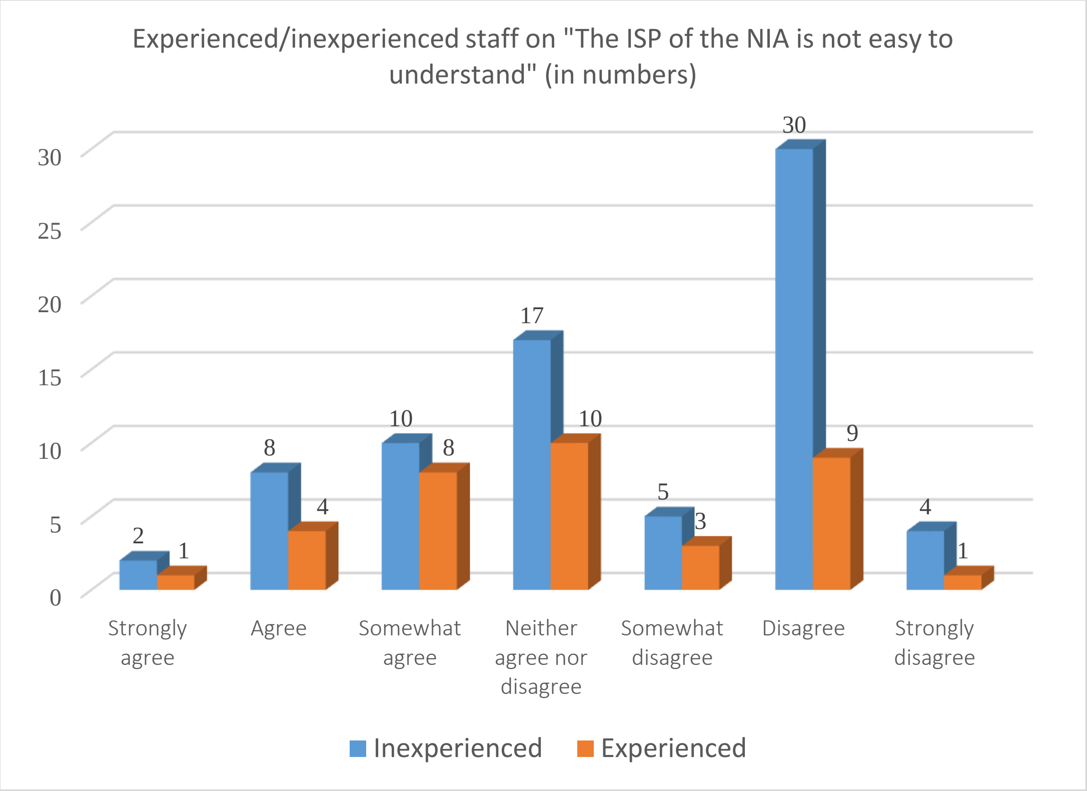


Figure 18: Graphical representation of years of work and "The ISP of the NIA is not easy to understand"

On the general disagreement of the NIA ISP not being easy to understand, a lot of them were new or inexperienced staff, as detailed below:

Gender	**Department**	**Years of Work**	**Employment Type**
Female	Operations	More than 9years	Permanent
Female	Operations	More than 9years	Permanent
Female	Human Resources	More than 9years	Permanent
Male	Finance	Less than 1year	Contract
Male	Operations	Less than 1year	Contract
Male	Operations	Less than 1year	Contract
Male	Other	Less than 1year	Contract
Female	Technology	Less than 1year	Contract

Female	Administration	Less than 1year	Contract
Male	Operations	More than 9years	Permanent
Female	Technology	Less than 1year	Contract
Male	Administration	More than 9years	Permanent
Female	Other	6-9years	Permanent
Female	Other	More than 9years	Permanent
Female	Operations	Less than 1year	Contract
Male	Technology	Less than 1year	Contract
Male	Technology	Less than 1year	Contract
Female	Operations	Less than 1year	Contract
Female	Operations	Less than 1year	Contract
Female	Operations	3-6years	Contract
Female	Technology	Less than 1year	Contract
Male	Technology	Less than 1year	Contract
Male	Technology	Less than 1year	Contract
Female	Operations	Less than 1year	Contract
Female	Operations	More than 9years	Permanent
Male	Technology	3-6years	Contract
Female	Technology	Less than 1year	Seconded

Table 8: Distribution for general disagreement category on “The ISP of the NIA is not easy to understand”

On “The ISP is easy to understand”, most of the operations and Technology and Biometrics departments agreed with the question. This is particularly true with “The ISP is practical” and “The ISP is reasonable”. Although the responses to all the questions are similar, it is essential to emphasise that they give different messages.

We also conducted a paired t-test to check the significance of the data. The results showed a significant relationship between the years of work and the content of the NIA ISP in terms of its understanding. The result is as presented below:

		Significance	
Question	df	One-Sided p	Two-Sided p
The contents of the ISP are easy to understand vs Years of Work	111	<.001	<.001

Table 9: Statistical Significance of ISP Readability

Attitude towards compliance vs Intrinsic Benefits and Extrinsic rewards

We assessed the relationship and significance of the attitudes of the NIA staff, their intrinsic benefits, and their extrinsic rewards, as detailed below:

Question	Category	Mean	Std. dev.
Attitude towards ISP compliance	Necessary	2.37	2.022
	Beneficial	2.37	2.022
	Important	2.01	1.663
	Useful	1.99	1.636
Intrinsic benefit of ISP compliance	Content	3.10	1.582
	Satisfied	2.88	1.425
	Accomplished	3.10	1.582
	Fulfilled	3.05	1.432
Extrinsic rewards for ISP compliance	Pay rise/promotion	4.41	1.858
	Personal mention/written assessment report	4.03	1.732
	Monetary/non-monetary rewards	4.60	1.867
	Tangible/intangible rewards	4.49	1.836

Table 10: Means and standard deviations for the survey questions

Attitude towards compliance vs Years of Work, Intrinsic Benefits and Extrinsic rewards

Question	Category	Experienced	Inexperienced

		Mean	Std. dev.	Mean	Std. dev.
Attitude towards ISP compliance	Necessary	2.33	1.690	2.38	2.172
	Beneficial	2.36	1.743	2.37	2.153
	Important	2.25	1.746	1.89	1.621
	Useful	2.31	1.721	1.84	1.584
Intrinsic benefit of ISP compliance	Content	3.81	1.833	2.76	1.335
	Satisfied	3.22	1.726	2.72	1.239
	Accomplished	3.33	1.773	2.99	1.483
	Fulfilled	3.36	1.693	2.91	1.277
Extrinsic rewards for ISP compliance	Pay rise/promotion	5.44	1.594	3.92	1.780
	Personal mention/written assessment report	4.81	1.582	3.66	1.686
	Monetary/non-monetary rewards	5.42	1.538	4.21	1.838
	Tangible/intangible rewards	5.22	1.623	4.14	1.838

Table 11: Means and standard deviations for the survey questions for experienced and inexperienced participants

Question	**T**	**Df**	**Significance**		**Mean Difference**	**Std. Error Difference**	**95% Confidence Interval of the Difference**	
			One-Sided p	Two-Sided p			Lower	Upper
Pay rise/promotion	-4.548	76.16	<.001	<.001	-1.523	0.335	-2.191	-0.856
Personal mention/written assessment report	-3.509	72.908	<.001	<.001	-1.148	0.327	-1.799	-0.496
Monetary/non-monetary rewards	-3.591	83.25	<.001	<.001	-1.206	0.336	-1.874	-0.538
Tangible/intangible rewards	-3.141	77.149	0.001	0.002	-1.077	0.343	-1.76	-0.395

Table 12: T-test for inexperienced vs. experienced staff for extrinsic rewards for ISP compliance

As noted, we classified the staff into two groups, experienced and inexperienced, based on the number of years they have worked for the NIA, with those working for three years or more classified as experienced and those for less than three years classified as inexperienced. From the above, the results reveal a significant difference in the mean responses of experienced and inexperienced employees relative to their perceived extrinsic rewards for ISP compliance. The inexperienced employees were neither in agreement nor disagreement, while the experienced employees were in disagreement.

Regarding the T-Test results, the difference between the experienced and inexperienced was statistically significant with $p<0.05$, as shown above (see Table 11).

Further to the above, from the Analysis of perceived intrinsic benefits of ISP compliance, we note that both the experienced and inexperienced employees generally agree. However, the inexperienced employees agreed more than the experienced staff, hence their lower means. Regarding its t-test results, only the difference for feeling content is statistically significant with a recorded p<0.05 (t=-3.05, df=53.233, one-sided p=0.002, two-sided p=0.004, mean difference=-1.042, std. error=0.342. and 95% Confidence Interval of the Difference (1.728, -0.357).

Finally, the experienced and inexperienced employees agreed with minor differences in their attitude towards ISP compliance. However, the t-test results show that the differences are not statistically significant.

4.5 Discussion

The outcome of this study is encouraging for the organisation, particularly for entities like the NIA. It underscores the necessity for formally approved Information Security Policies (ISP) that specify employee awareness, compliance, and enforcement strategies requirements. The significance of staff training is also highlighted, enabling employees to fully appreciate and understand policy provisions, while recognising the importance of organisational context during ISP development and implementation.

4.5.1 ISP Awareness

Despite the absence of a formally approved ISP and enhanced staff training on information security, the study shows that employees believe they know and understand what is expected of them. Increasing the confidence level of employees towards compliance and awareness can be achieved through a combination of a formal ISP and relevant staff training. This approach can further strengthen the information security culture of the NIA, which is crucial for EIS organisations.

These findings align with existing literature, which emphasises the importance of awareness and understanding in effective ISP implementation. For instance, studies by Siponen et al. (2010) and Ifinedo (2012) highlight that higher levels of awareness and understanding among employees lead to better compliance with information security policies. Additionally, best practices in information security management, as outlined by the ISO/IEC 27001 standard, stress the need for continuous education and training to maintain high levels of awareness and understanding. Additionally, Taylor et al., (2020) assert that education and training must consider other key stakeholders and actively engage them to prevent them from becoming liabilities. Training also seems to impact on knowledge and perceived information security Awareness of people (Farooq et. al., 2015).

4.5.2 ISP Communication

Effective ISP communication is supported by literature, such as the work of Puhakainen and Siponen (2010), which emphasises the importance of clear and consistent communication in fostering compliance. Best practices also suggest using multiple communication channels and regular updates to ensure all employees are well-informed.

4.5.3 ISP Readability, Reasonability, Practicality, and Comprehension:

Ensuring that the ISP is clear, reasonable, and practical is essential for fostering compliance. This is supported by literature, such as the work of Puhakainen and Siponen (2010), which emphasises the need for ISPs to be user-friendly and practical to encourage adherence. Best practices suggest involving employees in the policy development process to ensure the policy is relevant and understandable.

4.5.4 Intrinsic Benefits of ISP Compliance

The findings indicate that most respondents perceive intrinsic benefits from complying with Information Security Policies (ISPs). These results align with existing literature that suggests intrinsic motivation, such as personal satisfaction and a sense of accomplishment, plays a crucial role in compliance behaviour (Herath & Rao, 2009; Ifinedo, 2012). The high levels of agreement among participants underscore the importance of fostering a positive organisational culture that values and rewards compliance, which is consistent with best practices in information security management (ISO/IEC 27001, 2013).

4.5.5 Attitude Towards ISP Compliance

The survey results reveal a strong positive attitude towards ISP compliance among the respondents. These findings are in line with the Theory of Planned Behaviour, which posits that positive attitudes towards a behaviour increase the likelihood of its performance (Ajzen, 1991). The high agreement rates suggest that respondents recognise the critical role of ISPs in safeguarding organisational assets and maintaining operational integrity. This recognition is crucial for the successful implementation and adherence to ISPs, as highlighted in the literature (Pahnilab et. al, 2007).

4.5.6 Attitude towards ISP Compliance and Perceptions of Intrinsic Benefits

The study found that NIA staff have a positive attitude towards ISP compliance and perceive intrinsic benefits, which are essential factors for compliance (Bulgurcu et al., 2010; Jai-Yeol, 2011). Both experienced staff, who benefited from a formally approved ISP policy and ISP awareness training, and inexperienced staff, who lacked these benefits, showed positive attitudes. However, perceptions of ISP compliance negatively impacted extrinsic benefits due to rigid government control procedures on financial and budgetary allocations. The lack of an officially approved rewards system for ISP compliance is a significant issue. Managers can offer financial incentives, but these must go through rigorous approval processes, making it challenging to implement such rewards.

Additionally, the statistically significant difference between experienced and inexperienced staff suggests that the lack of clarity on extrinsic rewards for inexperienced staff might be a factor. Intensive awareness training for inexperienced employees could address this issue. Informal rewards, such as positive mentions in personal or written assessment reports, are not common in the NIA, as management emphasises deterrence.

4.5.7 Common ISP Violations

The research analysis highlights that staff understand common ISP violations and appreciate their roles and responsibilities in protecting NIA information security, indicating a good security culture. However, the level of agreement with ISP violations is not as strong as with other aspects. Differences in responses suggest typical tensions between security and usability, such as the inconvenience of logging out or locking workstations and creating complex passwords. Training employees on strategies to manage these tensions can help address these issues. The absence of a formally approved ISP means employees might be unclear about what constitutes careless use of laptops. A transparent and straightforward ISP, with clear guidelines on “do not bring-your-own-device” expectations, can help prevent compromised organisational security (Van Der Schyff et al., 2023).

In addition, the analysis of common ISP violations reveals three primary areas of concern: information transfer, password management, and workstation security.

- Information Transfer-Related Violations: These findings are consistent with the literature, which emphasises the risks associated with improper handling of sensitive information (D’Arcy & Hovav, 2009). Best practices recommend the use of encryption and strict access controls to mitigate these risks (NIST SP 800-53, 2013).
- Password-Related Violations: These results echo the well-documented vulnerabilities associated with poor password practices (Florêncio & Herley, 2010). Implementing strong password policies and regular training on secure password management are essential best practices (ISO/IEC 27002, 2013).

- Workstation-Related Violations: These behaviours pose significant security risks, as highlighted in the literature (Siponen & Vance, 2010). Best practices recommend enforcing automatic screen locks, secure configuration settings, and user awareness training to address these issues (SANS Institute, 2014).

4.5.8 Extrinsic Rewards Mechanism

The research highlights the need to improve the organisation's extrinsic rewards mechanism by providing more clarity to new staff and adopting a balanced approach between deterrence and rewards. Effective measures require a nuanced understanding of the motivations and precursors of insider threat behaviours (Renaud et al., 2024). Additionally, research on workplace rewards highlights the importance of balancing deterrence and rewards to enhance motivation (Thibault and Whillans, 2019; Beck-Krala, 2020). Effective reward systems should, therefore, be clear and integrated into promotional decisions and financial reward systems to encourage compliance and positive behaviour. Introducing compliance as part of promotional decisions and financial reward systems for staff can enhance motivation.

4.5.9 Broader Implications for EIS Organisations

For EIS organisations, the findings emphasise the importance of ensuring clarity on extrinsic motivation for ISP compliance through formally approved ISP policies. Compliance monitoring and ISP awareness training should be conducted for new employees, as attitude, training, intrinsic motivation, and other social factors can promote a positive security culture (Warkentin & Johnston, 2010). Further research is needed to establish the right balance between rewards and sanctions.

4.5.10 Findings on SSI

The study's findings highlight concerns about data ownership and control. Issues of data sovereignty, digital sovereignty, and self-sovereign identity (SSI) are significant due to security and privacy concerns about personal data (Tan et al., 2023). Creating an electronic identity (eID) to ensure higher privacy preservation has been proposed.

4.5.11 Data Sovereignty

Data sovereignty refers to individuals' right to control personal data collection, ownership, and application within a geographical location (Kukutai & Taylor, 2016). Due to increasing organisational globalisation and interconnection, data security and privacy have become more complex. Data should be governed by regulations specific to the region from which it originates and the country where businesses are conducted to avoid fines and criminal charges (Tan et al., 2023). Understanding data sovereignty can be based on principles such as Collective Benefits, Authority to Control, Responsibility Ethics (CARE), and Findable, Accessible, Interoperable, and Reusable (FAIR). These principles aim to advance legal principles underlying collective and individual data rights and maximise data use and reuse (Tan et al., 2023).

Regarding regulatory requirements, data sovereignty is closely linked to the laws and regulations of the countries where data resides. Ensuring that sensitive and private data are protected to remain under the control of their owners in a country or geographic location is crucial, guided by privacy regulations, best practices, and guidelines (Tan et al., 2023).

4.5.12 Digital Sovereignty

The EU Federal Chancellery (2020) opines that Digital sovereignty describes the ability to shape digital transformation in a self-determined manner regarding hardware, software, services, and skills. It does not mean resorting to protectionist measures but making sovereign decisions about areas where independence is desired or necessary within the framework of applicable law. Digital sovereignty is a key issue of concern and a challenge in the digital economy and society, despite its economic, social, and political impacts (Tan et al., 2023). While digital transformation aligns with the power of data for organisations, businesses, and governments, individuals often lack ownership and control over their personal data, leading to privacy and sovereignty issues (Couture & Toupin, 2019).

Digital sovereignty must emphasise citizens' autonomy in discharging their responsibilities as employees, consumers, and individual users of digital technologies and services, enabling them to decide who gets access to and uses their data (Pohle & Thiel, 2021). It is necessary to have control over the ownership, custody, and utilisation of data and to protect digital assets and identity through proper data governance, cybersecurity control, and privacy protection (Tan et al., 2023).

Digital sovereignty is still a relatively new topic, with recent discussions focusing on its execution and corresponding implementation technologies, infrastructures, and cloud platforms (Tan et al., 2023). This aligns with Christopher Allen's vision of "Self-Sovereign Identity" (SSI), which addresses digital identity issues and internet identity (Allen, 2021).

Self-Sovereign Identity (SSI)

As data owners, individuals are concerned about their data rights and control regarding usage and sharing (Pohle & Thiel, 2021). The increasing demand for sovereignty over digital identity has led to research on SSI, a new decentralised identity model that aims to solve digital identification and authentication problems and give individuals full control of their digital identity (Tan et al., 2023). Digital sovereignty should focus on individuals' ability to take a conscious, deliberate, and independent approach to handling and accessing their data (Pohle & Thiel, 2021; Geisler et al., 2021).

SSI enables individuals to have autonomy and control over their identity and personal data, with self-determination on the level of data to be shared, used and handled (Tan et al., 2023). SSI has potential applications in areas such as healthcare, finance, and government services, where securely managing personal information is critical.

Overall, the survey results provide valuable insights into the perceptions and behaviours of internal stakeholders regarding ISP compliance. By aligning these findings with existing literature and best practices, organisations can develop more effective strategies to enhance compliance and mitigate security risks. This research, using an EIS organisation as a case study, has therefore contributed to understanding the perceptions, beliefs, and concerns of Junior and middle employees as internal stakeholders.

4.6 Concluding Remarks

This chapter discusses the quantitative report from the junior and middle staff survey. It discusses the questionnaire designs, procedures and participants for the study and the study's analysis. It finally discusses, in detail, the demographic and non-demographic results of the study and its discussions. The research generally provides some essential considerations for electronic information systems during the details of an effective ISP. We did this by analysing the extent of involvement of NIA Junior and middle employees in the policy development and implementation processes, as well as their attitudes towards compliance and enforcement of their organisational information security.

The study also revealed the need for critical considerations in developing an ISP for Electronic Identity Systems. Key among them is the need to recognise both staff perception about ISP issues and real ISP issues in such organisations. Eg. On ISP Awareness, the staff that disagreed across the three ISP questions were the more experienced staff. However, they were in the minority (9% on ISP knowledge, 13% on ISP understanding, and 17% on ISP responsibilities).

This means that there is a need for the NIA to address this trend by urgently formalising the approach they use to train their employees and enhancing ISP awareness in the organisation. This is to prevent the tendency for such staff to influence the other staff in the organisation.

On ISP's most common violations, the study revealed that when the NIA staff say they know the violations, it is true that they know and understand their roles and responsibilities regarding the violation. However, they are less confident to say it.

The study revealed that the females responded less positively than their male counterparts to the ISP's most common violations. Further, the experienced staff are more optimistic about the ISP violations.

On ISP Readability, the study revealed that most of the staff that disagreed on “The contents of the information security policy are easy to understand” were permanent staff from the Operations and Technology and Biometrics departments. The majority of those who remained neutral on this question were permanent staff. This means there is a need to have a formalised ISP and a training programme for the staff to ensure adequate understanding and compliance with the NIA ISP.

For employees' attitudes towards compliance, we observed that the experienced staff were more negative than the inexperienced staff. Again, we observed the need to make the ISP of such organisations less technical. For instance, we observed that the operations department staff recognised the need for and use of an ISP but indicated that it was less necessary and beneficial to them.

On ISP Rewards, the permanent staff disagreed with the questions. This calls for the need for NIA management to carry out reorientation as well as instituting specific measures such as awareness training, incentivising the staff and seeking the inputs of the staff in reviewing the policy to improve compliance in the organisation.

Finally, On ISP Intrinsic Rewards, the experienced staff tend not to agree with the ISP Intrinsic Rewards questions compared to the inexperienced ones.

The next Chapter will focus on the study on the NIA Management views that we conducted.

5 Study 2 on NIA Management Views

The previous chapter discussed the general understanding of junior and middle staff on their ISP as internal stakeholders and emphasised the need to recognise their perception and reality of EIS ISP enactment, development and implementation processes. It also highlighted the need to ensure employees' compliance through motivation and sanctions, awareness training and the formalisation of the organisation's ISP from the junior and middle staff perspective. This chapter, therefore, focuses on the senior management perspective (management and Board of Governors members) of the NIA as internal stakeholders and their perceptions and thoughts about IS effectiveness, IS management and ISP. The chapter starts with the aims and objectives of this study, followed by the study design. It also provides insights into the methods, participants, and procedures used for the research work. It then provides a detailed analysis and results, followed by a discussion of the findings. It ends with a concluding remark on what the chapter covered.

5.1 Study Design

As indicated in Chapter 3, to answer the research questions in the context of EIS from the senior management perspective, we designed a semi-structured interview guide that focused on the importance and concerns about Information Security and its Management, ISP development, implementation and evolution relative to compliance and enforcement.

More specifically, we posed questions to assess their perception of the NIA ISP by interviewing them on the development and evolution processes as well as the effectiveness, importance and status of their policy as part of our attempt to find answers to the following sub-research questions:

> **RQ1:** How effectively are the NIA Information Security Policies protecting its Identity Systems?
>
> **RQ2:** What are the management members' views and thoughts about Information Security in Identity System Organisations?
>
> **RQ3:** To what extent is the management involved in developing, ensuring awareness, compliance, enforcement and evolution of Information Security Policies in Identity Systems?

5.2 Participants and Procedures

5.2.1 Participants

We targeted all past and present management members of the NIA for this study. Management members were those who had headed a department of the NIA or had been part of the governing board of the NIA. To this effect, we sent out 15 copies of invitation letter from the head of the Strathclyde CIS Department to the management members and board members (both past and present) out of the 22 members for their participation based on a distribution formula. The distribution formula was developed primarily based on the number of departmental heads and board members who have served or are currently serving as heads of departments or the board.

However, due to Covid 19 restrictions and the time limitation, we could interview nine (9) senior members of the NIA to elicit their responses as set out in the interview guide. Due to frequent organisational changes common to African governmental organisations, we focused on participants from different departments. We had past and current department heads, Executive Secretaries and board members/chairpersons as participants.

5.2.2 Study Procedures

As noted in Chapter 3 in the study and procedure section, ethics approval was obtained from our Department’s Ethics Committee before the study. We also received approval from the NIA to engage the management of the NIA (see details in Appendix 9.4).

Again, as noted in the methodology chapter (chapter 3), the interview session for each participant was face-to-face, and each of the nine participants lasted a minimum of 45 minutes (see details in Appendix 9.9a). The interviews were conducted at NIA and other agreed locations. In the case of the serving management members, we conducted it in their offices at the NIA headquarters in Accra. In the case of the past management members, it was conducted outside the NIA headquarters. In general, we completed the interviews between 14/02/2020 and 20/10/2020. The long length of the data collection was due to the Covid-19 restrictions. After the interviews, we transcribed them with the “Temi” software and used the NVIVO software for further analysis. Using the NVIVO software, we coded the responses into themes. As noted in the participant's section, we used a distribution formula developed primarily based on the number of departmental heads and board members who have served or are currently serving to ensure fair participation from each department.

5.2.3 Pilot Study

We conducted a pilot study with five research students in our department. We asked for their feedback, which was used to improve the study design before the primary data collection exercise. This uncovered some minor issues related to the structure of the questions, identification of some ambiguous questions, and testing of the results. The problems identified were all corrected. The pilot studies lasted for about 50 minutes for each participant.

5.3 Analysis

As indicated in Chapter 3, we developed a semi-structured interview guide to elicit responses from the respondents on the three broad categories, which were Information Security Effectiveness (Effectiveness), Information Security Management (IS Management) and Information Security Policy (ISP) (see details in Appendix 9.5). We also conducted a thematic analysis using the questions we asked to identify the themes and sub-themes under each category and then matched the codes to them. Each of the themes is described below under their categories:

IS Effectiveness

1. General: This covers general comments and recommendations on IS effectiveness.
2. Improvement: This covers suggestions on how to improve IS Effectiveness.

ISM

1. Effectiveness: This covers the participant's concerns and beliefs on information security effectiveness within the IS management context.
2. Emphasis: It covers vital information that provides some significance to the research within the context of IS management, such as other roles and beliefs.
3. Responsibilities: It covers the respondents’ belief on where the responsibility of managing IS lies, their primary responsibilities, and the other roles of the respondent in the organisation’s organogram.
4. Senior Management Roles: deals with the responses of participants on the role of senior management in securing the organisation’s information.

ISP

1. ISP Awareness: ISP Awareness is about mechanisms and approaches to orienting, educating and informing employees about the NIA ISP. ISP awareness generally entails the development challenges, management and mechanisms used to notify staff of the organisation's ISP awareness programme status.
2. ISP Content: The ISP content is about the legal and security provisions made in the ISP to protect the organisational resources such as the system, software, hardware, equipment, network, personnel and environmental factors.
3. ISP Development Process: This theme covers the processes and personnel involved in developing an effective ISP for the organisation. The ISP development process focuses on the development process, those involved in the development process, challenges to the policy development and the role of senior management in the development process.
4. ISP Enforcement: This theme discusses employees' understanding of strategies and approaches relative to compliance awareness, enforcement, and monitoring. It entails sub-themes such as compliance awareness, enforcement, monitoring and status of the NIA's ISP.
5. ISP Evolution: This theme concerns reviewing or updating the policy to suit the organisational needs that have changed over time. The theme encompasses sub-themes on the challenges, participants, senior management roles and effectiveness of amendments to the organisation's ISP.
6. ISP Importance: This theme covers respondents' beliefs on the general importance or need for the organisation to have an ISP.
7. ISP Status: This covers the respondents' views on whether an ISP exists in the organisation.

Apart from ISP Importance and ISP Status, each of the themes had sub-themes, as detailed below:

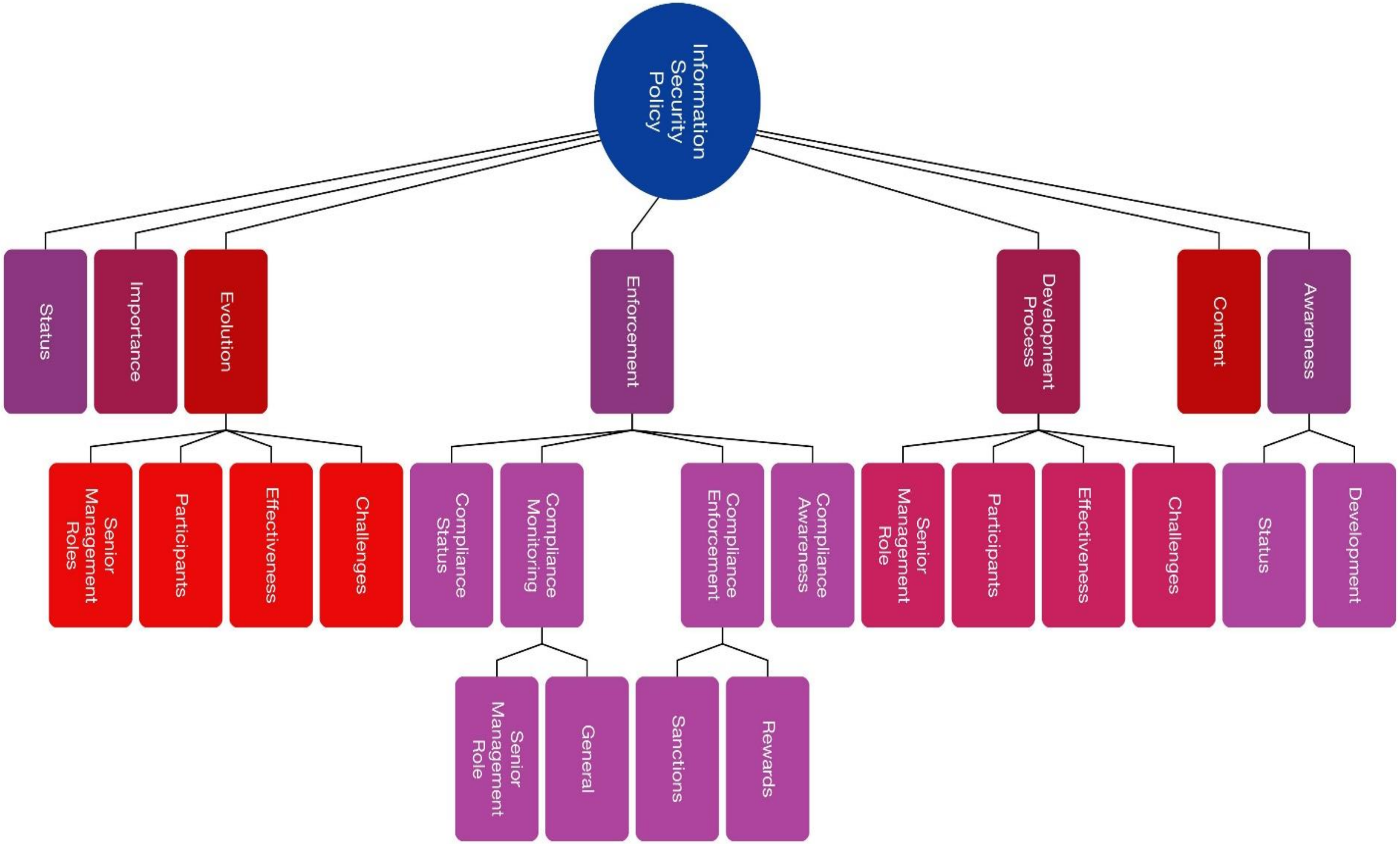


Figure 19: ISP Category, themes, subthemes and subtopics

To further synthesise the data, we adopted a bottom-up approach to group similar and different codes, making meaning from the data and answering the research questions as detailed in Chapter 3 (Section 3.2).

After synthesising the data, we confirmed the research findings by verifying and validating the codes and themes to ensure they accurately represent each respondent.

5.4 Demographic Results

The results section is divided into two main groups: demographic results and non-demographic results. The demographic results covered the participants' demographics and their primary responsibilities in the organisation. Table 12 provides an overview of the participants' demographic data as detailed below:

Participant Id	**Designation**	**Role**	**Duration**
P1	Serving Management Member	Admin	1-2 years
P2	Serving Management Member	Facilities	10-12 years
P3	Former Board Member	Board Chairman	5years
P4	Former Executive Secretary (CEO)	Executive Secretary	2-4years
P5	Former Executive Secretary (CEO)	Executive Secretary	2-4years
P6	Former Management Member	Legal	7-9years
P7	Serving Management Member	Internal Control	10years
P8	Serving Management Member	Tech	7-9years
P9	Serving Management Member	Tech	2-4years

Table 13: Demographic Distribution of Respondents

From Table 12 above, the participants were both management and board members (past and present) with responsibilities ranging from Executive, administrative, legal and advisory roles. Interestingly, some respondents have served in two different roles within the organisation. In terms of years in their positions, it ranged from one year to 12 years.

On other positions served, some of the respondents indicated the internal roles they played before they moved to different roles. For instance, respondent P2 states, *"I was the first Director to head the card production that is the printing of the national ID card".*

P5 also notes*, "I became the head of the IT (Technology) department then eventually I became the chief executive on the 15th of June 2015 until February, 2017"*. P6 also adds, *"I also had the opportunity to hold other titles including that of oversight for Administration and HR*

(Human Resources) for a number of years before reverting to my position as head of Legal and compliance".

Other respondents were sourced externally before they were given internal roles in the organisation. For instance, respondent P5 states, "*I was the consultant first. I became the manager of AFIS (Automated Fingerprint Identity System). I started in NIA in September 2009, and I finished, or I left NIA in February of 2017. That's how long I was there"*.

5.5 Non- Demographic Results

The non-demographic results were categorised under three main sections for effective presentation, which included:

- Information Security Effectiveness (Effectiveness),
- Information Security Management (IS Management) and
- Information Security Policy (ISP)

5.5.1 Research Categories

The research analysis yielded 14 themes (2 for the IS Effectiveness category, 4 for the ISM category and eight for the ISP category) as detailed below:

- Information Security Effectiveness (IS Effectiveness): The focus of IS effectiveness is to understand the general understandings, views and suggestions of respondents about the NIA's information security. To do this, we categorised the IS effectiveness under two themes: General and Improvement.
- Information Security Management (ISM): The ISM focused on respondents understanding and views about the security and management of both data and systems. The IS Management was categorised into five (5) themes: effectiveness, Responsibilities, Challenges and Senior Management Roles.
- Information Security Policy (ISP): The focus of the ISP is to understand the views and perceptions of respondents about the NIA's ISP development, implementation and evolution processes. To do this, we categorised the ISP findings under eight (8) themes that evolved from the data, which included ISP importance, ISP Status, ISP Awareness, ISP content, ISP Development Process, ISP enforcement, and ISP evolution.

We used the Treemap below to show the relative composition of the research's categories, themes, sub-themes and sub-topics. The Grey colour shows themes and sub-themes that fall under ISP. Interestingly, the data treemap shows that the ISP category was the most dominant in the research, followed by the ISM category. The ISM themes and sub-themes were shown with brown colour and the least dominant component in the research data was the blue colour that represents themes and sub-themes under the IS Effectiveness category.

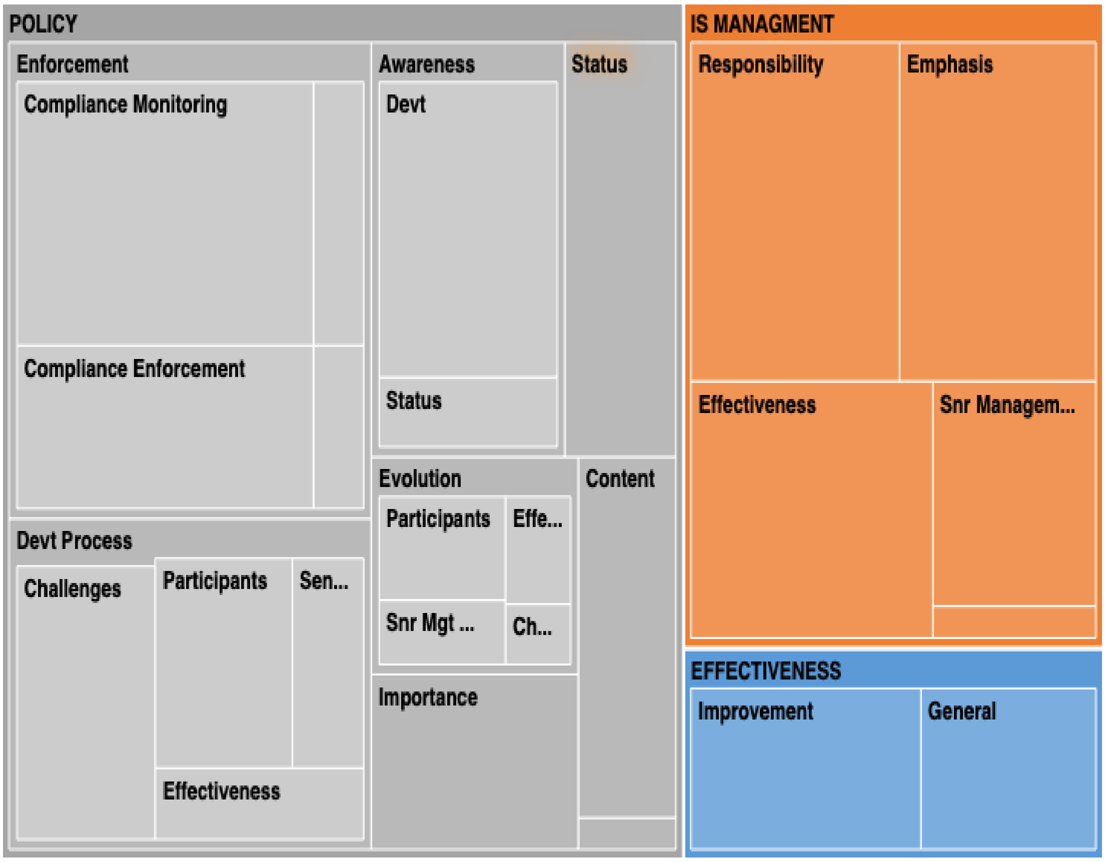


Figure 20: Treemap showing components of categories, themes, sub-themes and subtopics

5.5.1.1 INFORMATION SECURITY EFFECTIVENESS

General IS Effectiveness

Respondents highlighted physical security, changing obsolete equipment, controlling and regulating information and using human and technical strategies ensure general IS effectiveness. Additionally, respondents believe in the need for positive attitudes towards compliance and prioritising data and security to ensure general IS effectiveness. P2 and P3 for instance, emphasise physical security for data and system protection and respectively state, "*There are some other areas if you don't belong there, you don't have access to those areas*" and "*And of course, we need to also introduce security cameras to track movement of people, particularly around your AFIS central database*".

Some also suggested that the items and equipment must be regularly changed and more advanced CCTVs installed. P1 stated, "*In the case of compromise, you need to gradually change and get a new set of items/equipment If we allow a system to be compromised*".

Some respondents indicate the need for controlling and regulating access to data to ensure the confidentiality, integrity and availability of information. On this, P3, for instance, observed, "*The key element is everything from physical security to data security. These are some of the elements of it. The system of controls, access to sensitive information has to be controlled and regulated*".

Regarding the human and technical Strategies, the respondents appreciate the need to protect the system using human and technical strategies to ensure ISP compliance. For instance, P1 indicated, "*We can ask our personnel to help protect the system if we talk to our personnel or we use our IT people to do that*".

P3 adds, "*The place was meant to be controlled in all aspects, including physical security. The security and physical security elements so on, all complemented the IT security systems. They all kind of integrated and all meant to be*".

Regarding system access, some respondents believe there is a need to ensure that there are restrictions on permitted access to the system and data. There is a need to make provisions or clarify the people allowed to access the organisation's data. This is to prevent both the data and system from damage and compromise. Respondent P1 states, "*Even from accessing the system, we have to put processes that will prevent other parties from assessing the system. It means if you are accessing the system, you need to pay for what you want. You cannot let everybody be on the system because some people will can damage the system if you allow them to penetrate your system. They can hack it*".

Positive attitude towards compliance: The respondents further acknowledge the need to ensure a positive attitude towards compliance among the staff to prevent compromise. More specifically, the respondents indicate that there should be rules to protect the data and the security of collected personal information due to its prime importance as captured under the sub-theme codes for data compromise on information security effectiveness. For instance, P3 states, "… *we considered the data to be of prime importance because essentially you're collecting people's personal information*".

P5 adds, "*I believe that some basic do's and don'ts are in place and in our time that was protecting information and security of individual information*".

The respondents also indicate the need to prioritise the security of the data and the NIS system and why it is right. Some asserted that, regarding physical security, the organisation must emphasise electronic and paper-based forms used to collect personal information and the filing systems in which the papers are stored. This is important due to the sensitivity of the data collected to ensure the data's confidentiality, integrity and availability. For instance, respondent P1 states, "*And then thinking about information securities (IS), IS is not only about machines. it also encompasses paperwork. You classify certain information*". The respondent, P1 even suggested that the collected information be classified into security levels such as confidential, secret, top secret and restricted by stating, "*You classify certain information: you have a confidential, secret, top secret, and then restricted. It's like a pyramid where you have the top secret and then top-down and the base would be restricted (restricted, confidential, secret, top secret)*".

Another respondent, P8, adds to the need for prioritising data and system security by indicating, "*When it comes to the systems side, there are levels. So you talk about the physical security, that is from the gate: the security men, the CCTV, you know, the surveillance system. And so all those things need to be stated clearly as to what is required from that point*".

Data Confidentiality, Integrity and Availability (CIA) is another observation from respondents. Respondents highlight the need to ensure that the data is available to the right people who are authorised to access it for the right reasons. P5 states, "*Information security should not be looked at only as prevention of information because getting it into the wrong hands is not the best. But the preservation of the information too, is information security. That's also a very important aspect, and therefore, how is redundancies built into the system to ensure that data integrity is intact?*".

Some respondents acknowledge that the CIA is not only about data and systems. The respondents believe that it should include human resource integrity and financial integrity. For instance, P6 states, "*I will be looking at a policy that has regard for system integrity, for human resource integrity and with financial integrity*".

On Funding, some respondents highlight that IS funding challenges affect the effective provision of security to data and system. P1 for instance, states "*Another challenge is if the*

NIA is not given funds to protect their system, it will be very difficult. If you have bought a very good new system where you store data and you are not able to purchase high firewalls to protect them, it means anybody at all can intrude and hack".

Some respondents also highlight that the leadership and their prioritising of IS plays a significant improvement in ensuring general IS effectiveness. P8 for instance states, "*I think the head (referring to the CEO or Executive Secretary) needs to take a bold decision. But it's like the management's priorities now, or the focus now is on other areas, especially making sure that we go to the field and collect the data before maybe we'll think of those issues. But I, being a technical person and someone who is very much into system security, I think it's a misplaced priority because security is considered to be part of the design: from scratch, when you are designing something, you need to consider security. You first need to do your assets assessment. The assets that you want to protect: is it a building? Is it the personnel or the officers? Is it the hardware? The physical? So, you do the assessment of your assets. You put values on them; you categorise them. Then, depending on the categorisation, those which have a higher risk determine what kind of provisions you need to put in place. Those are the medium risks, and it follows to the lower risks*".

Improving IS Effectiveness

Regarding improving IS effectiveness, the respondents indicated that policy compliance, training, education, and employee orientation on essential security matters can improve it. For instance, P2 stated, "*The policy has to be followed because, for me, if we are IT-driven, everybody has a laptop, everybody has a password that he can use to go into whatever system they have in the policies*". At the same time, P5 adds that "*they are also impressed upon to ensure that they adhere to the tenants of the policy so that information is not compromised*".

P4 and P5 also respectively say, "*Everybody had to go through basic training in programming and I.T forensics so that you at least do some basic things*" and "*And once everybody accepts it, adequate training is given to them to ensure IS effectiveness".*

On education, orientation and education, P2, P4, P5 and P8, for instance, stated the following:

- *P2: Education should be big among the stakeholders and the commitment, and then the drive from the government to secure the system.*
- *P4: Staff would also have to be oriented as to what to do to protect people's data.*

- *P5: A lot more would have to be done, a lot more education would have to be done to ensure that it is so tight that nobody's personal information can fall in the wrong hands.*
- *P8: Because the human is the weakest link, So if they are not well educated, they are not well sensitised, they can easily be a threat. They can easily be used to circumvent the system.*

The research also highlights the need to adopt technical and physical protection strategies to improve IS effectiveness. For instance, the respondents emphasise that password changes every six months [though against the latest password management advice], restricting staff access, networking the system encryption, and firewalling are some of the technical strategies to help protect the system. On this, for instance, the following responses were recorded:

- *P2: Every Six months, you change everybody's password, then you are going to try to secure the information.*
- *P4: You have to introduce levels of encryption along the network so that nobody can hack into it and steal anybody's data.*
- *P4: The systems that you introduce should be robust enough to be able to prevent attacks by firewalling it against any hacking attempts.*

In terms of the improvement in physical security, some of the respondents such as P1indicated "*We have directed that people do not to use their pendrives on office machines. We should be able to block such acts of picking off information in a way that you cannot copy from one system to another*".

The respondents also suggested adopting control measures and involving experts in the IS effectiveness activities, which could help improve its effectiveness. For physical security, some of the views are listed below:

- *P2: We'll do what we call access control. So if you're on first floor, you can not just get up and go to second floor.*
- *P6: It also needs physical security in terms of access to the data system where it is kept; who works there, what goes in there. And yes. So those are some of the things that need to be enhanced.*

- *P9: We are trying to implement an Access control system in the building where each floor is restricted. If you work in this floor (referring to 2nd floor), you cannot have access to the next floor.*

On the involvement of experts, the following were some of the highlights:

- *P2: The intellectual aspect is getting the experts to sit down and put all these structures in place.*
- *P4: What you need to do is you bring in technical people who can then serve as the institution's board, and then they control all these other institutions, which by law are supposed to be subordinated to the authority on biometric register.*

Finally, the respondents also recommended further career training of qualified technical staff as a motivational tool to ensure enhanced compliance and data security in the organisation. For instance, P4 states, "*Those who demonstrated some capabilities went on to do further programmes or training*".

5.5.1.2 INFORMATION SECURITY MANAGEMENT:

From the management perspective, the respondents assert that effective IS management involves ensuring the effectiveness of the system and data, clarifying and supervising the IS roles and responsibilities of employees towards the organisational plans, goals and objectives. Generally, the ISM, according to them, is to ensure the achievement of system, network, physical and data security by ensuring that there is necessary administrative support, legal compliance, and trustworthiness through collective and individual roles of the employees and other recognised stakeholders. To better understand Information security management from the perspective of the respondents, the following four themes from the data are discussed:

ISM Effectiveness

Respondents were asked about their views on how the NIA prioritises its ISM. The respondents highlighted that in their views, they believe that the NIA must consider it to be prime or a high concern to manage the NIS effectively. They believe that the prioritisation would help in achieving the organisation’s mandate. The respondents also justify that the prioritisation of ISM is necessary to address some administrative concerns, system and data security concerns, and legal and regulatory concerns thereby immensely helping in the organisation's security management. For instance, some respondents indicated that an ID system organisation should consider ISM prime and protect their system and data. On administrative concerns for example, P2 states: "*These [some of the ISM issues] are purely administrative challenges. And a commitment from the chief executive and the administrative sector. Because we have to have people who can sit down and follow up this with the public service commission for the condition of service to be properly approved*".

On system and data security, another respondent, P1, states, "*Everybody looks to NIA as the main source of reckoning their identity. You have a lot of people who have registered to this system, and if the system is not well protected, is not well preserved, we will have ourselves to blame because we should not compromise the system*".

On legal and regulatory concerns, respondent P7 adds that "*it is in a sense that, we keep personal data and we are to protect this data. For instance, now because of the current data protection laws and all that, we have to be very very careful about the data that we keep here. So we need to come up with a security arrangement in such that these data that we collect and keep are protected*".

Some also believe that the effectiveness of the ISM is necessary and justify that it is a requirement for consideration when an ID organisation is to be considered for an international standard organisational certification. For instance, a respondent, P4, stated, "*It is important. It's so crucial, so critical. It's so important that we actually worked towards getting an international standard organisational certification to protect the data that we have*".

Some respondents also believe the ISM effectiveness contribute to ensure the system's robustness, data transmission and sharing. For instance, P4 states, "*for an ID management institution, one of its core responsibilities is to ensure absolute protection of the data that it has in its care. That is its core mandate in terms of data transmission and data sharing, and in my time, we were quite robust. Because all of those systems that you see there were done in my time*".

Again, the respondents acknowledge that ISM's effectiveness is achieved by preventing unauthorised access to data, thereby ensuring confidence and trust. For instance, a respondent, P3, asserts that "*If you want people to have confidence in the system, if you want businesses to trust the data for verification and other things, then there should be no doubt in anybody's mind that that data that they are accessing is correct and not accessible to a* *wrong person. If they can hack the system to get the president's data or they will get other people's data, they can do all kinds of things with that*".

In addition, the respondents were of the view that such concerns would affect effective ISM in the NIA as P2 stated, "*the management of it is critical because if it goes out into the wrong hands, we there know that it's going to be like people's personal information being out there and being misused*". P2 further explains, "*So if somebody volunteers his personal data for you, that is, he is put his own life into your hands. You cannot play with that data, like I said, and other organisations are looking for that*".

Another respondent, P8 adds that ISM effectiveness is "*a major concern because somebody trusts you and he entrusts his information to you for keep and to manage. That is, they have entrusted that consent to you. So the responsibility is huge on you as an authority, or as people who manages the process to make sure that, that trust which has been handed over to us by the individuals that we are keeping their identity or information. There' should be no or any compromise in terms of data breach or in terms of their data being tampered with. So it's a huge responsibility*".

Further to the above, the respondents emphasised the need for the organisation to operate within the existing legislative and regulatory frameworks such as the data protection law. P5, for instance, emphasises this when he asserts, "*Basically, handling people's data falls under the data protection laws that in this country exists, and you need to comply with and how you handle personal data and for which purpose you are keeping or taking that data. And it should be very clear to the person who is giving his information to use and feel so freely that this is the purpose for which you are using it*".

Another respondent focused on the restrictions that management faced because what the organisation does should be supported by an adequate legal basis. On this for instance, a respondent, P2, states, "*We have to have a legal backing. You can't just get up and change certain things. So, the parliamentary aspect is very critical. We have to get it into the parliamentary service so that they pass it through the normal procedure to have it as a bill and then L.I (Legislative Instrument) or whatever you can call it. That's critical*".

This means that laws related to data protection and the restrictions that the law poses to such organisations need to be factored in when developing an ISP or an IS management Plan to make it more effective.

Finally, the respondents highlighted the need to monitor the “big” interests of the public-private partners and their staff in Identity management organisations to prevent bribery and corruption, informal controls/professional misconduct of management members, data leakage, identity theft and other compromises. As noted in Chapter 3 on the NIA, the public-private partnership helps ensure both the NIS management and the issuance of biometric cards to citizens and residents. The respondents stated the following:

- *P1: The private partner has a very big interest, his first motive is to buy in key responsible officers who are supposed to safeguard the government entities.*
- *P2: For my own personal view, I can say that there are some guys who are selling information. There are people who came here from the private side, they just virtually walking, but now they are buying cars all over the place and they have access to the data” and “So due to the sensitivity about the data, national ID or national data should not be in the hands of the private entity all the world over”.*

ISM Responsibilities

On the ISM Responsibility, the analysis focused on two key areas: where the responsibility of IS management lay, and the primary duties of the respondents.

On where the responsibility of IS management lay, the respondents generally indicated that the management of IS lies in the organisation's managers. Most respondents indicate that IS management responsibility lies with Technology and Biometrics and some of them include P1, P5 and P9 as highlighted below:

- *P1: It is the Director of Technology and Biometrics who has to ensure that and then of course, supported by the Head of Administration and the Executive Secretary.*
- *P5: The technology department was tasked with the additional responsibility of ensuring that there's information security. So the entire security setup was split into two: Physical was handled by operations and then, information security, was handled by the technology department.*
- *P9: The department of technology and Biometrics is in charge of the information security policy being supported by the private partner.*

However, the rest do not endorse the belief that the Technology and Biometrics department is responsible for ISM. They either see that it as the responsibility of other departments or the Executive Secretary. Some also see it as the responsibility of the private partner and NIA management. Some also see it as a Board responsibility or an organisation-wide responsibility. In specific terms, the respondents views are as follows:

First, P2 and P8 believe that the Executive Secretary is responsible and state that "*It purely comes to the figurehead, the head of the entity, the Executive Secretary*" and "*It has to be the chief executive officer himself. He has to be the one that is in charge of information security*" respectively.

P4 thinks it is the CEO and the Technology and Biometrics and states, "*The Chief Executive is the ultimate, but we had the director of I.T (Information Technology and Biometrics) that handled the technical bit*".

P7 indicates that it is with the Board of Governors with inputs from units and management and states "*Ideally it should rest in the information security policy and every information security policy issue, in fact has to come from the top governing boards. Even though it has to be done and prepared by the various units, .I mean by management, the approval has to come from the top management, that's the Board*"

P6 believes it is an organisation-wide responsibility starting with the Board and states "*It is an organisation-wide responsibility starting from the board. In fact, you can even bring in the minister who has oversight over the policy directives for the organisation, through the board, to management and to every member of staff who works there because every person's role impact on the management of the organisation in one way or another so it is something that has to be cascading from the top, all the way to the bottom*".

The respondents also acknowledge the roles of the various departments and why the ISM is a collective responsibility of senior management. For instance, P6 states, "*It's a combination of every sector, every department coming together to play their roles in ensuring that the organisation meets its security policy concerns and their objectives*".

Finally, the respondents indicated that the Senior Management must provide resources for ISM and endorse such plans. For example, P9 states, "*The Senior management have to provide all resources to enable the unit to function to its best level*" and adds, "*The senior management have to endorse this policy developed by the department to support this approach*".

On the primary duties of the respondents, the respondents generally indicate that the management members play critical roles in ensuring information security management. The respondents indicated that their primary responsibility included the administration of policies, facilities management, executive management, technical field operations, and systems update, legislation and legal advice, compliance and setting policies and providing organisational policy directives. P1, for instance, relate to the administration of the policy and states, "*I am the Administrator and Head of Human Resource, to administer policies and generally look at the affairs in the house concerning procurement, facilities building and general administration of the NIA*".

P9 adds, "*I am the head of technology and biometrics units. This means that I head the biometric aspect of the business*" and "*I also head the technology aspect of this business in terms of management, in terms of policies, in terms of implementation processes, approaches to achieve things. So these are the high-level things I do*".

On facilities management P2 for instance, state "*I'm a deputy director since 2012 and am the head of the facilities department. So I'm the property manager*"

On the executive management, P4 state, "*I was the chief executive of the authority from August 2009 to April 2013 and so I actually ran the organisation for that period"* and "*So the responsibility of a chief executive is to just superintendent over the performance of the authority's Mandate*". P7 adds, "*My main responsibilities for this job is of Internal Audit. And its function is to carry out audits and professional evaluations of the activities of the authority. And to ensure that the system of internal controls applicable to financial program and project areas provide reasonable assurance. And to ensure that the management and the financial, managerial and operational information reported internally and externally is accurate, reliable and timely*".

On technical field operations, and systems update, P8 states, "*My responsibilities is to be in charge of the data centre and also when it comes to the field work, I'm the technical coordinator for all the field technical related incidents and activities. So basically I manage the machines and the technical staff on the field. But at the main office, I am in charge of the data centre and ensuring that the various systems are, the uptime is maintained and also everything is working how as supposed to be*".

On legal advice and development of Legislative issues, P6 states, "*I was in charge of Legal matters. So I gave advice on legal matters that affected the work of the organisation. So it's basically giving legal advice and legal support to the Authority*".

On ensuring compliance, P7 adds, "*We also ensure that the financial activities of the authority are in compliance with applicable laws, policies, plan, standards, and procedures. It is my responsibility as the head of internal audit to ensure that national resources are adequately safeguarded, used judiciously and for the intended purposes. Also, plans, goals, and objectives of the authority are achieved*".

On setting policies and providing organisational policy directives, P3 notes that "*I was the Chairman for the Board of Governors or Board of Directors of the National Identification Authority. I was appointed around late 2010 as the chairman of the Board. I served up to the late part of 2015". "As the chairman of the Board, my main responsibilities as I understood was to chair the Board of Directors meeting and to ensure that we were responsible for setting policies, directions for the NIA and also making sure that NIA fulfills its objectives under the NIA ACT, the ACT that established the National Identification Authority*".

ISM Challenges

On the ISM challenge, the study shows some unique challenges due to the nature of the organisation as a public sector organisation and the political context within which it operates. These challenges would require taking a holistic view of information security, instilling an information security culture, developing comprehensive information security policies, and ensuring policy compliance.

Additionally, the NIA struggles with aligning its information security policies with relevant legislations, managing relationships with other government stakeholders and private sector organisations, and operating within government constraints. On political interference for instance, the respondents noted that through political appointments and government funding of equipment, the governments controls the effective management of the organisation. A respondent P2 states, "*This is where we have a very huge government issue. And this one, I will chip in. Politics is also changing the civil service face, but it has its own negative side too because we have all these political figures being thrown into the system who more or less seem to be the one who wants to work for the face of the company".*

P3 adds that *"The French, Sagem Morpho were the technical advisors, technical supporters, suppliers of the system and they were also finding it difficult to access their money from the Government. The real challenge was that by the time when the money came through, the technology, the equipment, the machine and all others were obsolete*".

Some respondents also identified that the provision of resources, personnel and funds by the organisation's leadership is a huge challenge. P6 for instance state, "*It must take leadership to say that we appreciate that situation and put everything, everything to resolve them in terms of resource, personnel, Funds. That will enable the policy to be implemented. In the absence of these, the policy will also suffer similar fates*".

ISM Senior Management Role

On the senior management roles, respondents highlight that the senior management role includes:

First, some respondents indicated that senior management is involved in monitoring the attitudes of personnel to ensure data security and general ISM. For instance, P4 states, "*The Senior management are supposed to monitor what is happening in terms of security of the data*"

Again, some respondents indicate that senior management report departmental security and ISM issues for management to resolve them. For instance, P3 state, "*Mostly there will be senior management as heads of department and up to the level of Chief Executive at the management level. We meet and they report to me [to the executive secretary] on what has been done*".

Further to the above, some respondents also explain that senior management plays the role of educating personnel and orienting them on their security behaviours and data handling to ensure effective ISM. On this, P1, and P5 for instance, respectively, state, "*You educate the people on how to put the systems in place and to prevent intruders from coming in. So basically, this is what the process should be from the senior management" and "The senior management are to talk to personnel working with them not to compromise the systems that they are using*" and "*It behoves anybody who is a leader at NIA, and by that, I mean a head of the department, and therefore responsible for staff to have that orientation that they are working within a security-driven institution and therefore behaviour and the way information is handled must mimic that of a security-driven institution*".

Some respondents also believe that the senior management serve as focal persons for employees to ensure ISM. For instance, P3 states, "*Well, the senior management are the primary focal persons*".

Enforcing the ISM rules and regulations is another senior management role identified by other respondents. They indicate that the senior management is responsible for the information security management within their departments through enforcing the ISM rules and regulations. For instance, P5 state "*Each head of department [heads of department make the NIA management] they themselves are more or less custodians and hold the responsibility of ensuring information security within their departments because NIA is a security-driven institution*".

Some respondents believe that the role of senior management involves ensuring the implementation of IS policy. On this, P6, P7 and P9 for instance state the following:

- *P6: Senior Management has the mandate to implement any security policy that we put in place. The Finance Department has to ensure that there are available resources of funding to ensure that there is a smooth sailing or implementation of any security policies. The IT Department have the mandate of ensuring that every plan, every strategy is implemented to the latter with a view to ensuring safety, security and confidentiality of the information that we have and have been entrusted to the organisation. So everybody has a role to play, even with procurement. Procurement may play a role in terms of what tools we need to apply or what we need to buy. So procurement has the responsibility to ensure that we get the best system possible for the organisation's operations. So it's a combination of every sector, every department coming together to play their roles in ensuring that the organisation meets its security policy concerns and their objectives.*
- *P7: As managers there, they have to make sure that the various rules or security rules and regulations governing that area are enforced or implemented" and adds, "It is our responsibility to ensure that the Authority has a security policy and that it is judiciously implemented.*
- *P7: Apart from that too, like I said, internal audits, we also monitor officers. And our role is to make sure that the provisions within the security policy is complied with. So it's like we just take the checklist and use that checklist to do our compliance audit.*

- *P9: The senior management is in charge of bringing in appropriate staff levels to man the department's units actually and the department concerned.*

Finally, respondents also believe that management has the responsibility of providing an effective ISM using an external expert. They do this through contracts. For instance, P9 highlights that "*So we are looking at finalising it [a contractual agreement] with a proper security firm [IT security firm] to produce the final document*".

5.5.1.3 INFORMATION SECURITY POLICY (ISP):

The ISP covered seven themes: ISP importance, ISP Status, ISP Awareness, ISP content, ISP Development Process, ISP enforcement, and ISP evolution. The discussion on each of the themes is detailed below:

A. ISP Importance

The ISP Importance theme covers respondents' views on the importance of ISPs. From the responses, participants indicate that ISPs have individual, organisational, national, and general benefits.

On the individual benefits, the respondents highlight that the ISP ensures the security of individuals' data and crimes related to identity fraud. For instance, P4 adds, "*If anybody gets hold of your identity, they can clean your accounts. They can commit crimes in your name. And they do a lot of other things. So the ISP is very, very crucial in this whole identity management environment*".

The respondents believe that the ISP can contribute to preventing employees from mismanaging individuals' data. An example is where P3 states, "*So if we wanted the whole idea of the national identity register establishment and so on to be accepted by the people, we understood very clearly that people had provided their data and must feel that their data was safe with us and would not be stolen or people would have access to it or to misuse it. The IS and the ISP were very important things for us to protect the data we had*".

The respondents also indicate that the ISP facilitates the provision of enhanced services to the citizenry. On this, respondent P4 stated, "*It's supposed to aid business, it's supposed to aid crime control, it is supposed to aid fighting money laundering and all of those things*".

Regarding organisational benefits, the respondents believe the ISP helps the organisation control, verify, and execute its mandate of providing secured data to other user organisations. For example, some respondents P4 and P6 highlight this by stating that:

- *P4: It was meant to be a complete system that will allow for business and for other services. That's why the security policy and security arrangements, encryptions are important even between the authority and the user agencies.*
- *P6: The ISP is the bedrock for securing a credible, independent and stronger organisation in view of the work NIA does.*

Further to the above, the research highlights that the reliance of external stakeholders on the NIA is part of the importance of the NIA as an organisation. P6, for instance, states, "*We are talking about the Ghana Immigration Service, Social Security and National Insurance Trust, the National Health Insurance Authority, the Ghana Statistical Service. In fact, they need data from us. Therefore, we expect that any policy document must have regard for their inputs so that those stakeholder concerns are taken care of*".

P4 adds, "*If you have committed a crime and that's reported to us [meaning to the NIA], and you are tagged, you can be stopped anywhere in the world. If you probably defrauded a bank and you are escaping, that can be checked easily*".

In addition, some respondents indicate that the ISP helps prevent crime and other forms of cyber fraud. For instance, respondent P4 states, "*If anybody gets hold of your identity, they can clean your accounts. They can commit crimes in your name. And they do a lot of other things. So the ISP is very, very crucial in this whole identity management environment*".

P4 adds, "*If you have committed a crime and that's reported to us, and you are tagged, you can be stopped anywhere in the world. If you probably defrauded a bank and you are escaping, that can be checked easily*".

On the national benefits of the ISP, respondents P1, P4 and P7, for example, show that the ISP helps to ensure the security of the data for economic, social and political purposes. Some of the comments are listed below:

- *P1: I believe that we really need to have an ISP because a lot of Ghanaians are hooked on to the system. And if we allow our system to be compromised, it will have a lot of impact politically, economically socially. It will affect us because we derive economic* *benefit, we derive political benefit and we derive social benefit. All these aggregate to help the nation in a way to let it develop.*

- *P7: The ISP is very, very important in the sense that the type of what we do, the data that we collect are people's information, their bio-data of millions of Ghanaians. So with these current technological advances, if you are not careful, someone can just use someone's bio-data to do some bad thing which won't augur well for the image of the Authority.*

B. ISP Status

Three observations could be drawn from the analysis of the status of the ISP in the organisation. The first group believes there is/was an ISP in the organisation. The second group believes there is no ISP, and the third group is either unsure of a policy presence or needs confirmation from others.

ISP Existence: On the existence of an ISP, some of the respondents, like P2, P3, P6, P8 and P9, believe that there was an existing ISP in the organisation. Some of the comments stated by respondents include the following:

- *P2: There's a security policy.*
- *P3: As far as I am concerned, I would say that that policy had been discussed and developed. The board approved it.*
- *P6: I would not say no because there have been various policies in the past that were looked at by management and approved for it to be implemented. So I won't say we don't have.*
- *P8: There was one that we were using. That was what the French people did for us.*
- *P9: Yes, the policy has been in existence, and we have amended it recently.*
- *P9: Yes, we have. So senior management have endorsed the policy and Approaches.*

ISP Non-Existence: On the non-existence of the ISP, P1 and P7 indicated that there was no policy in the organisation. Some examples of their comments include:

- *P1: I have not chanced upon any document which talks about Information Security Policy.*
- P7: *Yes. So, as of now, if anybody tells you we have a security policy, it is not true. I can show you the audit report on that. I can even show you the outstanding issues, and they are still outstanding. Even though to say that we don't have a security policy*

in this house (referring to the organisation) should be surprising and an embarrassment for someone to hear that.

Needing further confirmation (General)

Some respondents were unsure of the presence of a policy or otherwise. P4 and P5, for instance, were uncertain of the existence of a policy. They state that:

- *P4: I began drafting that when I left. I don't know whether it was completed, but essentially everybody is aware.*
- *P4: I am not sure whether it's not been finalised.*
- *P4: I'm not very sure what they have there now.*
- P5: "Well, let me say that we were not there yet. There was a lot that could have been achieved. Things were not as tight as it was supposed to be. So, I would say that a policy was in an infant state. I don't think the board had approved the security policy of NIA."
- P5: "Well, let me say that the board had granted some interim approval and had recommended that we deal with some few institutions to beef up the security policies. That's how we left it. So with that, I think there is not much to be done now. But of course, everybody has a new ideas they can bring on board and therefore they could look at the draft and then recommend your own changes".

Needing some work: Despite the varied positions on the existence or otherwise of the policy, some of the respondents' comments show the need to clarify or update the status of the organisation's ISP. Some of the comments were as follows:

- *P1: I can only check to see whether we have an Information Security Policy. If we do not have, then there is the need for E9 (Management member) and co to develop one.*
- *P2: During the first founding father, I saw some policies drafts but that's to say his term didn't actually end in a way that he could probably have finished all these things like a document for NIA. Whether he gave it back to NIA, I'm not sure. Whether he took it away is another thing because he's an intellectual. He probably might have done that.*
- *P2: We don't have a document that says that every management member even has a say, this is our policy, this is what we are going to do and teach all the staff, etc. For*

that, I haven't seen it yet. And currently, here is also such that is like the current crop of chief executives are more into executing than building the structures or creating a system in an enabling environment where everybody could work.

- *P4: I began drafting that when I left. I don't know whether it was completed.*
- *P4: I am not sure whether it's not been finalised".P4: "I'm not very sure what they have there now.*
- *P5: Well, let me say that we were not there yet. There was a lot that could have been achieved. Things were not as tight as it was supposed to be. So, I would say that a policy was in an infant state. I don't think the board had approved the security policy of NIA.*
- *P5: Everybody has a new ideas they can bring on board and therefore they could look at the draft and then recommend your own changes.*
- *P7: As at now we don't have information security policy. It's a draft, it's a draft. And the management has not finalised on this draft. Management has to finalise on it.*
- *P9: I came to meet it [referring to NIA ISP], but then when I came, we have actually worked on it [the NIA ISP] as a department, and so it does not follow any. We are still looking at working on it to make it [the NIA ISP] better.*

C. ISP Awareness

To better appreciate ISP awareness, we identified sub-themes from the participants' responses. The sub-themes included ISP Awareness Development and Awareness status. Under ISP Awareness Development sub-theme, we assessed the development challenges, and development management. From the participants' responses, we can say that the NIA management's understanding of ISP awareness is about orienting, educating and informing employees using various communication approaches such as information screens, durbars, workshops, seminars, and departmental meeting notice boards. The details of the sub-themes are as below:

- Awareness Development

Challenges: On ISP Awareness Development Challenges, some respondents emphasise that the NIA should explore practical ways of delivering information to employees, especially on the organisation's ISP. Some respondents indicated how the NIA fails to circulate or inform staff about the existence of the NIA ISP. An example is when a respondent, P1, sums it up by stating, "*Failing to circulate or failing to inform them that this policy exists and that they should not do this or they should not do that is another challenge*".

Some respondents also note that the ISP awareness challenge is due to the absence of a formally approved ISP that clarifies the ISP awareness structure, the entire organisational governance process, and the political interests of management and other corporate leaders. A respondent, P5, observes and indicates that the organisational structure contributes to the ISP awareness development challenges by saying, "*It was just because it hasn't been fully finalised. That is why it wasn't rolled out. So therefore, as the board had given some interim approval, I think it is the political will of the people, the management and leaders of the place to ensure that it is trickled down to the rest, the ordinary person*".

Management: On ISP Awareness Development Management, the respondents indicate that, after educating employees, there is the need for their understanding to be tested to establish whether or not they know what they are supposed to do to protect the data and the system. P1 asserts, "*After educating them, you need to test them to see, you need to find out whether the training that they had they have really understood it by observing their behaviours, their attitudes in the office and whether they are doing what they are supposed to do"*.

Again, respondents also indicated that the management must have a commitment and administrative guidelines and procedures to assess employees' awareness levels, as that would help manage some compliance issues. They believe this could be done by getting the Public Service Commission to approve it per the organisation's condition of service document. For instance, P2 indicates, "*These are challenges that are purely administrative. And a commitment from the chief executive and the administrative sector. Because we have to have people who can sit down and follow up this with the public service commission for the condition of service to be properly approved*".

The respondents also assert that the constant provision of relevant information on security awareness is another mechanism to ensure effective ISP awareness. P6, for instance, is of this view and indicates, "*The managers have to keep on giving their subordinates the relevant information so far as security awareness are concerned in each sector. It is the heads in the various sector. It is their responsibilities to make staff aware of the security arrangements and can make it known to them*".

The respondents recommended that the organisation uses durbars, circulars, memos, screens, seminars, billboards, brochures, mini posters and workshops to increase staff awareness P2 states, "*Corporate affairs department in the case need to have some communication outlets like seminars, workshops etc to create awareness*". P2 adds, "*So first of all, the communication aspect is important. This is what we want to do, so you do that through billboards, memos, seminars, workshops or, brochures or mini posters. This creates the awareness and then see how everybody fall into the fold*".

- Awareness Status:

On the awareness status, the respondents indicate that circulars, memos and staff durbars are used to interact with and educate staff on policies in the organisation. For instance, a respondent, P1, asserts, "*On awareness, we use circulars, and here we don't have screens where when you pass around, you see the information on the screen. So circulars, memos, for now, are used to create staff awareness*". Participant P2 adds, "*Staff are also educated about their conduct, the sensitivity of the information they work with, and all of these kinds of policies*".

Other respondents believe that they expect the management to drive the organisation's awareness of the ISM. For instance, P8 and P9 state, "*They have to drive the process. They have to get the people [staff] involved, educate them, and create awareness. Because when you see your head or your management member being part of the process, they themselves getting involved, it will be easy to pull along the junior and the lower ranked staff*" and "*They have to educate them through communication and awareness creation. That's what the senior management has to be in charge of that*" respectively.

In addition, some respondents indicate that staff orientation, incentivising employees, and upgrading their skills help with awareness creation among the staff in the organisation. On orientation and skills upgrade, for instance, a participant states, P4, "*We have tools such as regular orientation, skills upgrading, general durbars that we had introduced and bring their brains to the notice, the need for protection*".

On incentivising staff, a participant, P5, highlighted that "*It's also important to incentivise them because most of their colleagues working other security-driven institutions have a certain premium on their pay because of that. So, incentivising them through the extra* *allowances that people working within such institutions and then educating them on what is contained in the policy and why the policy is designed that way is helpful*".

The respondents also added that the publication and synthetisation of policies to departmental notice boards, vintage points and operational manuals help increase staff awareness. On this, respondent P6 shares his view that they ensure awareness "*Through staff durbar, through publications and synthesising. Assuming the document is huge, synthesising them into small write-outs for staff to be able to digest very easily and having some of them spread out on notice boards and at various vantage points for staff to be able to see it on a regular basis*".

A respondent, P9 adds that though the awareness is not up to expectation, they could use awareness and education to ensure awareness among staff by stating "*They have to educate them through communication and awareness creation. That's what the senior management has to be in charge of that*".

D. ISP Content

The respondents' view on the NIA ISP content shows that an EIS ISP like the NIA ISP must focus on critical issues such as software security, personnel security, employee conduct, data sharing, employee motivation, policy management and satisfactory legal & statutory requirements. In addition, the respondents indicate that the ISP should focus on stakeholders' relationship management, making provision for other recognised approved administrative documents as well as dealing with identified content constraints related to ISPs.

On software security, the respondents note that educating the personnel on conduct and minimising information security vioations must be part of the organisation's ISP content. For instance, a respondent, P1, states, "*The personnel working on the equipment is to be educated. They need to ensure that nobody tampers with the system. The use of passwords also requires that you minimise the number of people that are to be allowed to work on it (the passwords) on a system*". Another respondent, P2, also notes, "*In the policy, I will look about the management of the password is one, the personnel, the grooming of the personnel, this communication that will go to them as to how they conduct themselves in their environment*".

On personnel security, the respondents believe that schemes and strategies for attracting and hiring personnel should be essential in the ISP content. This, they believe, would make the employees more effective and would make the organisation hire the best personnel for the organisation. For instance, respondent P6 states, "*Beyond that, there has to be provision for ensuring that we have the best personnel NIA can get to work for the organisation. We have to ensure that the quality of personnel is perfect. For instance, we have to ensure that the personnel are qualified, they have integrity and are patriotic, knowing that the job they are doing is very, very important*".

On policy management, the respondents highlighted the need for constant policy review updates, stakeholder consultation and practical enforcement guidelines. More specifically, the respondents believe that the content of the NIA ISP must have information on the policy content and how such policy contents are regularly reviewed to match with technological changes. P6 notes, for instance, that "*We also need to ensure that constantly, its security policy is reviewed and there is a provision in the contract that makes provision for this review to be happening on a regular basis*".

Other respondents suggest that the policy should cover the access rules and employees' conduct. For instance, P5, states, "*Who, and for what reason, for what purpose is it allowed for them to have access to other people's otherwise private or privileged information? All these things can come into play. What is the conduct of the people within the area, the do's and don'ts that will ensure that information of individuals remains private to those individuals?*".

On the content of ISPs, the respondents note that the policy should also specify what is shared with internal and external partners. Respondent P7 states, "*It should have something on data sharing because at least we, as an Authority, are obliged to share data with other institutions. I think we are to share with some organisations (external organisations), and there should be some security provisions around that, and there should be a provision on what type of information are we supposed to share*".

The respondents also believe the policy should contain directives on how to manage the organisation's relationship with external partners. For instance, a respondent P7 states, "*Within the Authority too, the data-bearing assets that we even have here, because we have a partnership here, Who should be in control if there's any external partner involvement here?*

What should he do? What should be his level of control? I think all these things should be factored in the information security policy here".

On employee motivation, the respondents highlight a need for a provision in the policy to incentivise or motivate staff compliance with the organisation's policy. A Respondent P6 states, "*I will be looking at a policy that has regard for system integrity, for human resource integrity and with financial integrity*".

Additionally, other some respondents noted that there is a need for management to motivate employees by providing non-financial resources. For instance, P9 notes, "*basically people were as well motivated not in terms of financial, but to talk them, to help them with resources to do the work. We provided them with concepts and approaches, website addresses to follow or to utilise so they could work through it*".

Respondents also highlighted that as part of the ISP content, the management members should be tasked or are tasked to enforce the policy guidelines at the departmental level. For instance, P2 states, "*If you are a manager, you have to enforce basic guidelines within your department*".

P6 adds, "*Well, policies in themselves do not enforce themselves. Somebody must be responsible for its enforcement. So that is the first thing that we need to admit. So you need the will and determination on the part of senior management*".

Regarding legal and statutory requirements, some respondents believe that EIS Policy content must be strictly done to conform to ISO27001 international standards. For instance, respondent P9 asserts, "*It touches on or follows ISO 27,001. Basically, that's our benchmark*".

In terms of ISP content constraints, some of the respondents believe that any policy that is identity-management focused must have clarity on the governance structure by taking into cognisance the nature and statutory requirements of such EIS organisations. For instance, P6 states, "*We need to put this within a context of what NIA does. NIA is an identity management organisation, so any information security policy has to have regard for that statutory mandate*".

On the administrative aspect of the policy content framework, the respondents indicated that fully approved ISPs should make provision for administrative and regulatory framework documents, such as the organisation's condition of service documents, to enhance the overall management of the ISP and staff compliance. A respondent explains that such documents like the Condition of Service document can be helpful in the skillset needed to drive the whole ISP development process. Respondent P2 states, "*So the skill sets and then the conditional service are properly mapped out so that the right skills set comes in, then the policy will drive the whole process because they just don't come in anyhow. That's my personal view*".

Some respondents also believe that the NIA added business continuity process provisions as part of their ISP content to guide organisational integrity of the NIA. On this, one respondent, P9, states, "*We have also worked on business continuity process as an aspect of the policy. That is something that will guide the integrity of the organisation to operate in case something should happen in there. So it's all part of it. It's all components of it*".

E. ISP Governance

On ISP governance, respondents believe that there must be collaboration with stakeholders to make inputs and develop the policy. A respondent, P6, indicates, "*This means that we must go beyond the four corners of these institutional representatives on our board and seek to have a national interaction by making other stakeholders who will have certain contributions to make. So based on their input, we can then sit down and fashion out the policy that takes the concerns of everybody into consideration. A policy that will also be forward-looking that will be visionary in terms of our work*".

Regarding governance enforcement, some respondents believed that adequate provisions must be made on enforcement strategies to ensure staff compliance with the policy. A respondent, P7, states, "*No matter how good a security policy is, if it is not enforced, it will not be a good policy in the public sector. Like every public sector, enforcement is always a problem. So in the security policy, in there, number one, top management must accept it. They must drive it before the lower levels will also take the security policy serious and they abide by the rules*".

The respondents also believe that since time is not constant, the ISP governance process is effective when organisations make provision to ensure a continuous review of the policy to meet the time needs. A respondent, P6, sums it up: "*The policy must address the needs of the time. Therefore, when the time changes, there should be change also in terms of how that policy is made and how there should be constant review, constant tracking, constant* *monitoring and of course, that will lead to continuous effective policy documents. So it is very important that we are constantly on top of issues locally and internationally and making provisions to the policy to go along with changes that happen*".

Some respondents note that, as part of the governance process, there is a need to develop reporting structures for the senior management to know their roles in monitoring the policy monitoring process. P9 also adds that the senior management has "*reporting structures being in place because senior management would not do the day-to-day work. Somebody has to be doing it and reporting or briefing like Regular meetings with the team or the unit to get a briefing on the ground and to also support with ideas on how best to achieve the final objective*".

F. ISP Development Process

The research identified sub-themes based on the views expressed by the respondents on the ISP Development process. These sub-themes included challenges of the development process, effectiveness of the development process, participants involved in the development process, and the senior management role in the development process.

- Challenges:

A challenge that the respondents believe hinders the development process of the NIA ISP policy is resource constraint. Respondents believe that it prevents such organisations from getting the right people to participate in the development process. The respondents' comments explains how funding, time constraints, cooperation, or lack of human resources with requisite expertise involvement influences the NIA ISP development. For instance, respondent P2, states, "*If you want to get people together to sit down, there must be some funding aspects. You don't just call people anyhow. And you've got to locate them somewhere and let them brainstorm. It is a brainstorm thing. You jig-jaw, and then you will find it. So funding is critical*".

Further to the above, another respondent, P9, adds to the funding issue by stating, "*We didn't have a budget at the time to take care of that [the development process]*". This means that the policy development process and IS management must be funded to ensure adequate security.

Additionally, some respondents believe that the NIA views the development of an ISP as technical and, as such, needs to have an internal expert to be involved in the development process. This is because the non-involvement of experts becomes a difficulty to the organisation in the development process. For instance, P9 notes, "*It was difficult because we needed the expertise. Some of them were thinking they could not do it*".

Regarding time constraints, some respondents like P7 assert, "*We don't normally have time to do other important things than to concentrate on the fieldwork. Those who are supposed to work on it [the development process] are all busy*". Another respondent, P9, adds, "*So another challenge was the timing [for the development process]. That was the time where we were doing all the planning activities concerning the mass registration. So Timing was the problem*".

Another challenge to the policy development process is the potential conflict of interest situation. Respondents acknowledge that some organisations that have representatives on the board of the NIA board and other user agencies started to compete with the NIA on their mandate by building similar biometric systems in the country. Here, the respondents note that it created an ineffective management board and conflicts of interest, as some of such organisations were to be part of the organisational ISP development process. A respondent, P4, states, "*Unfortunately for us, these institutions were represented on our board, the governing board. If you have situations like that, that they are developing their own ID systems, biometric databases, when ordinarily they should be drawing on the data within the authority, you run the risk of your data being compromised. This is because the board that's supposed to make policies for the authority and board members have on their own organisations, also building biometric databases. So there was conflict of interest when they are creating their own databases and they are the decision makers of the authority, you will have a challenge [in developing and approving the NIA ISP] there"*.

Another challenge of the development process is the non-prioritisation and the willingness of management to develop an effective, well-approved policy for the NIA. The respondents believe that the desire for leadership and, by extension, the management poses a significant challenge to the ISP development process. For instance, a respondent, P6, states, "*I do not think the challenge is about formulating the policy. There is a lot of documents out there that can be used for such a policy. So, the challenge rather for me will be the will to formulate one.*

The will to get the policy approved and taken through stakeholder engagement and the will to implement the policy".

- ISP Development Effectiveness

On the ISP development process effectiveness, the respondents view highlight having a national interaction with stakeholders outside the organisation facilitates the development process. For instance, P6 states, "*This means that we must go beyond the four corners of these institutional representatives on our board and seek to have a national interaction by making other stakeholders who will have certain contributions to make. So based on their input, we can then sit down and fashion out the policy that takes the concerns of everybody into consideration. A policy that will also be forward-looking, that will be visionary in terms of the work that we do*".

Some respondents also indicated that the involvement of experts would enhance the effectiveness of the ISP development processes. For example, P3 justifies this by stating, "*Right from the inception, we got a group of experts together to formulate our own data protection theme. We had a group of people to begin the processes for discussing the policy and also coordinating with the ministry at that time*," and P4 adds, *"We got together a team and fortunately for us, the company that supplied the main equipment were from France and was on a contract. They also exercise some proprietary rights over some aspects of the system. And therefore we had to work in collaboration with them to develop the data protection and Data security systems*".

Respondents further believe that as part of the development process, EIS organisations must have provisions in the policy to stop any other government institution/competitors from collecting the personal data of citizens and residents to prevent wastage and duplication of data. This they believe would enhance the development process effectiveness. A respondent P4 states, for example, state "*If I have a problem with any institution creating a national biometric database against what the law says, I should get my board to stop them or take them to book. Now it is the board members [that are spearheading the development of new policies to empower them to build their own systems*]".

Respondents also identified that the involvement of the staff in ISP Development process enhances its effectiveness through discussions and seminar training. Respondent P4, for instance, indicates, "*It [the ISP development process effectiveness] involves discussions, it* *involves the installation of systems, and it also involves practices of accessing the data. We did all of that. And then it involved training because the equipment is supplied by a particular company, and so we need to do some training for those who are going to manage that. Part of that training involved the technical handling of the equipment and also data protection arrangements. So all of these things went into the processes that we introduced in developing the policy*".

Other respondents also indicated that the involvement of quality personnel with a sense of integrity and motivation by the management of EIS organisations helps to make the development process more effective. A respondent P6, for instance, asserts, "*We have to ensure that the quality of personnel is perfect. For instance we have to ensure that the personnel are qualified, they have integrity and are patriotic, knowing that the job they are doing is very, very important*". The respondent further explains, "I*f you have a demotivated, frustrated, hungry staff, there is a danger to the integrity of the system you are going to put in place. So I will be looking at a policy that has regard for system integrity, for human resource integrity and with financial integrity*".

- ISP Development Process Participants

On Participant Involvement in the ISP Development Process, the responses highlighted that three categories of participants are involved in the ISP development process: the organisation's internal stakeholders, government, and other external stakeholders.

Regarding the internal stakeholders respondents believe that internal stakeholders like the NIA's junior and middle staff and management members must be involved in the ISP development process as participants. A respondent, P5, for instance, highlighted this by stating, "*It's not just the senior management because if you are developing these things and you don't include the junior and middle management, you will be making a mistake*".

P3 adds, "*The process was basically the involvement of the key stakeholders both internally and externally Internally with the key departments Technology Department Operations, management in general". And Externally, other user agencies for discussions, seminars, exchanges*".

P6 also adds, "*Everybody that works for the organisation is an internal stakeholder as far as I am concerned, so they have a stake in the effective and efficient functions of the NIA by reason of their employment*".

P8 states, “*If I say everybody matters, it has to start from the lower rank to the top because information security is about the people. So if the very people that are supposed to live by the policy and you don't involve them, it becomes a problem*”.

P9 also noted that the process should include “*All of us. All the key people in the department were involved*”.

Despite the above, some respondents believe that a few individuals or departments within the internal stakeholders must be involved in the initial development policy process. They explain that the few could develop the policy based on the needs of the organisation, and when they are unable, then there will be the need to bring in other experts or individuals. On this, P7 states, “*In fact, the relevant units have to come out with these needs requirements. Then if there is the need to bring in external experts to help, then they will maybe help to sharpen it*”. Another comment was, “*I'll say largely that it is the head of Bio and Tech (Technology and Biometric Department). Then addition to the key is head of operations, head of Internal Audit, Head of Finance as well as the head himself (referring to the Executive Secretary), he should be the champion the Executive secretary. And any other relevant units, but these are the key areas*”.

Regarding the external stakeholders involvement, the respondents also believe that the government and government-appointed private partners will be involved in the development process. On this, for instance, a respondent, P2, observes that the private partners, appointed by the central government to the NIA under a public-private partnership, participate in the development process by stating that, “*Currently the NIA with this Dermalog Project and the PPP (Public Private Partnership) are here as we are doing the development of the policy*”. Another respondent, P9, adds that the development of the policy was done through a combined effort between the NIA and the technical partners by stating, “*All of us [in response to the question on who were involved in the ISP Development]. All the key people in the department were involved. And the technical partners. It was a combined effort*”.

In terms of government involvement, P2 says, “*Again, with the process, I can't be too sure how it should start, but it should start from the government*”.

As noted above, interestingly, some respondents believe that the government's direct involvement as a participant is vital in developing such policies due to their funding role for such EIS systems and the systems’ public interest nature. For instance, P6 explains that based on the public interest nature [using the taxpayers money to fund such systems, the public takes interest in how their data and money are utilised], their interest and participation is to be noted in the development process of the ISP. P6 states, "*But above all, the public-interest nature of the work that we do must be taken into recognition*".

Other external participants according to some respondents, are involved in the development process. They mentioned external institutional stakeholders. According to them, such organisations are involved because the data is essential to their operational and lawful responsibilities. Respondent P2 states, "*We need a Nita [National Information Technology Agency is the agency responsible for implementing Ghana's IT policies]. We need an NCA [National Communication Authority to regulate telecommunications in Ghana by granting licenses for operation, ensuring fair competition among licensees, monitoring the quality of service, setting equipment standards, protecting consumers by providing safeguard mechanisms and coordinating frequencies with neighbouring countries]. We need the SSNIT [Social Security and National Insurance Trust undertakes several roles: It replaces some of the workers' lost income in Ghana due to invalidity, old age, or death of a member where dependents receive lump-sum payments. It collects contributions from registered employees and pays pensions and other benefits]. We need the DVLA [Driver and Vehicle Licensing Authority was established in 1999 by Act 569 of Ghana's parliament. The act allowed the authority to have a semi-autonomous status in the public sector organisation under the Ministry of Transport. The authority is responsible for ensuring safety on Ghanaian roads by promoting good driving standards in the country and ensuring the use of roadworthy vehicles on the road and other public places]; and we need the NHIA [National Health Insurance Authority was established under the National Health Insurance Act 2003, Act 650 to ensure access to basic healthcare services for all Ghanaian residents through the National Health Insurance Scheme (NHIS). All residents are eligible to subscribe to the scheme by paying a subsidised premium]. We need a Controller and Accountant General Department [CAGD acts as the Chief Accounting Office of Government and advises the Government in matters relating to accounting. The office carries out revenue monitoring and accounting in ministries, departments and agencies (MDAs) and other arms of government to ensure uniformity as well as formulate the Accounting policy of the State government, payment of all government employees and servicing of public debt and loans]. I mean, all of these stakeholders that we have. Immigration [Ghana Immigration Service Act of 2016, Act 573 is to ensure the application and enforcement of laws relating to the immigration and employment of non-*

Ghanaians in the country; manage and patrol the borders of the country;] for example, Police [Ghana Police Service is mandated to protect life and property, prevention and detection of crime; apprehension and prosecution of offenders; preservation of peace and good order and enforcement of all laws Acts, Decrees and other regulations with which it is directly charged.], especially because if this card become very usable in future and the police stops you asks you where your card is and you produce, they should be able to verify and see your DVLA details. These stakeholders are part of it because it also affects their work and the people they deal with".

As noted further by P3 earlier on the internal stakeholders in the development process, it also acknowledged the involvement of user agencies for discussions, seminars, and exchanges, among others.

Some respondents even explain further that it is because of the importance of the NIA data to the operational roles of such institutions that the government, through a legislative instrument (LI), made some institutions part of the NIA Governing Board. A respondent, P6, for instance, indicates, "*Therefore, we expect that any policy document must have regard for their inputs so that those stakeholder concerns are taken care of*".

The respondents indicated that aside the institutional members and other known government agencies, professional data management organisations like Sagem Morpho, France, among others, were involved or must be involved in the development process of the NIA ISP. P4 affirms this by stating, "*And therefore they [Sagem Morpho, France] needed to be part of the development of that whole, even though some didn't have I.T backgrounds. So, they became part of the team that helped in developing a policy*".

Respondents also acknowledged the involvement of Ernst and Young, in the development process of the policy. P3 explains, "*So right from the inception, we got a group of experts together to formulate our own data protection theme. We had a group of people to begin the processes for discussing the policy and also coordinating with the ministry at that time. The French, Sagem Morpho, were the technical advisors, technical supporters, suppliers of the system and we involved them". P4 adds that "And then we worked with a local firm, Ernst and Young, their role was to work out the structure of the policy document*".

- Senior Management role

Regarding the senior management role in the ISP development process, as noted earlier, P1 and P8 respondents for instance believe that senior management must educate themselves and their subordinates about the policy development process and the need to protect the data and the system.

In addition, other respondents note that the senior management role is to ensure that everybody in their unit or department is involved by contributing to the development process of the ISP. A respondent, P8, for instance, states that senior management "*has to take the responsibility of ensuring that everybody's involved in the process and their contributions are well considered and well documented. So they have to actually drive the process*".

Other respondents believe the senior management role should include making inputs to the ISP development process. On this, a respondent, P7, indicates, "*Senior management, since they will be working with the policy, they need to have inputs, and every unit head will help design the development needs of each sector. And these inputs from heads in a way will contribute to the development of the security policy*".

Some respondents also believe that the senior management role in the policy development includes providing policy proposals and endorsement reports for the Board of Governors' consideration and approval. One respondent, P5, notes this by saying that senior management "*First of all, they have to, of course, they would receive policy direction from the board. And most of the time, it's not the board actually giving direction because it's a bottom-up approach. Management will come up with the security policy [draft security policy]. But technically speaking, it should be coming from the board. So they draft the policy for approval by the board*".

Regarding the policy endorsement proposal in the development process, a respondent, P9, states, "*The senior management have to endorse this policy developed by the department to support this approach*".

G. ISP Enforcement

This theme deals with the employees' compliance awareness, compliance enforcement, compliance monitoring and status of the NIA's ISP. Generally, the participants' responses indicate that their understanding of an ISP enforcement process ensures compliance in the organisation with the sole objective of protecting the NIS system and data. To achieve this objective, the respondents believe there is a need to enforce the ISP by making all stakeholders aware as well as monitoring their activities. The respondents also believe rewarding or sanctioning the employees, when appropriate, promotes compliance. To provide clarity, we will attempt to discuss each sub-theme in detail.

- Compliance Awareness

First, the management views indicate that educating or orienting employees contributes to compliance awareness. For instance, a respondent, P4, states, "*Once you take them through these processes unless when new people come, you have to orient them towards what is operating in the organisation*".

Further to the above, some respondents observed that making the ISP policy document available to employees and appraising them on the ISP document contributes to effective ISP compliance awareness. On this, a respondent, P6, asserts, "*You make the document available to staff, you do the special courses, you review in terms of appraisal of staff on their Knowledge of the document and how they tried to work with the document as they are working in the organisation. So through the appraisal system, through the refreshment courses and yeah, these are some of the ways one can use to ensure that staff are made aware of the policy*".

- Compliance Enforcement

On ISP Compliance enforcement, the study noted that awareness, such as ensuring compliance, oversight supervision, education and communication, and regulatory compliance, helps in general ISP enforcement. Under the compliance enforcement, there were two sub-themes identified, which included Rewards and Sanctions, as analysed below:

First, regarding rewards, some management views indicate that writing to acknowledge someone positively influences ISP compliance enforcement. A respondent, P1, for instance, notes, "*You have to write a letter thanking him and indicating that what he did was good or writing a letter to commend him*".

Some management members believe that providing tangible or intangible rewards to employees facilitates ISP compliance and enforcement. For instance, the respondents believe that selecting and sponsoring employees for further training could motivate other employees to put efforts into complying with the organisation’s ISP. On this, a respondent, P2, states, “*Somebody can go for two-week training outside and in his job area. Because then it means that such a person understands what we're doing. So what do you do? So, two weeks somewhere, even in Canada or Ghana. It's a reward because he's add-on and he can be useful to those who are with him. When he comes back, he doesn't keep to himself*”.

Some respondents also suggest that an annual award for general security behaviours is an innovative way to support ISP enforcement efforts. P4 and P7, respectively, state *“that would be something that an organisation would do if maybe Annual rewards for ensuring that data is protected and not breached or something, that can be done*” and “*through a rewards schemes implemented in the Authority. So normally, inside reward schemes, it is normally done by management. Maybe management is saying that each department head should come up with a nominee for that award*".

Some respondents suggested general motivations like giving recognition and other in-house forms of awards to the employees to prevent a breach of confidentiality, breach of privacy, unauthorised access, and unauthorised disclosure to ensure enforcement. On this, P6 explains, “*And then internally, reward can also be enhanced through the various ones in the conditions of Service and other internal documents. Of course, then you may not have a reward system in laws but you may have a reward system within the organisation where people who excel, who will help the system to perform well are recognised and given awards*”.

Regarding general compliance, P6 asserts the need to give the best position to employees with integrity and notes that the employees “*are given the best position one can never find given our situation because if you have a demotivated, frustrated, hungry staff, there is danger to integrity of the system you are going to put in place*”.

Regarding sanctions, some respondents believe that there should be sanctions as part of ISP enforcement to ensure ISP compliance. The respondents also think that the punishments can be minor or major depending on the level of violations. Key sanctions highlighted include warning letters, suspension, interdiction (half salary), demotion, dismissal and a jail term. For instance, on suspension, dismissal and warning letters, P1 and P7 state, "*Suspension, dismissal and warnings letters will be given to offenders*” and “*If it is a major offence, staff will be expelled or sacked. One can be interdicted*” respectively.

P9 also adds, "*Suspension can be one of them. Total dismissal after successive or excessive repetition of the same crime or error. It's also part of it, and yeah, suspension on different periods depends on the crime's strengths or the disobedience*".

On half salary (interdiction), suspension, or dismissal, another respondent, P6, also states, "*The sanctions could be anything that was rightly written down within the conditions of service such as half-monthly pay or suspension, or depending on the gravity of or the impact of what is done to compromise information security. So it could range from anything up to a summary dismissal*".

On demotion/surcharges/transfers, respondents P2 and P7, respectively, suggest. "*If somebody is not compliant, you take him out and send him somewhere that he cannot be a threat to the security of the data because he's not compliant. So it's not like you are sacking him, but unless it is very grievous but, you will take him out. It is a demotion, and you lose that power of being strong in that area. Then you are clear of having the proper security checks in place*" and "*But minor offenses, there's a reduction in rank or surcharges*".

On the jail term, P2 and P4 state, "*You can go to jail. If we establish clearly that you've breached the security arrangements, you can be prosecuted. And the law actually states that if you try to register twice, it is a breach of our security. You can also be punished by law*" and "*Like somebody stole 60 laptops recently, he is in court. In such situations, you may go to prison*".

In addition, some respondents suggest that sanctions should be based on other relevant statutory laws related to identity management organisations. On this, respondent P6 and P7 supported this. P6 for instance states, "*One way to look at it is the point of view of what the sanction in lieu is in terms of violation of the relevant data protection Laws and other I.T Laws. That is one way. It can also be looked at from the point of view of employment contracts. You can also specify them very clearly in various employment contracts for people in what we call the Conditions of Service. That document spells out do's and don'ts as far as the policy is concerned*".

P6 explains that sanctions can be looked at from both law and regulatory perspectives by stating, "*sanctions can be looked at in these two ways: in the statutory way in terms of the Laws and regulations. In the NIA laws, there are various sanctions regimes for breach of confidentiality and breach of privacy, unauthorised access, unauthorised disclosure, etc.*

There are also some in the Data Protection Act. So from the statutory point of view, it can be looked at in terms of these laws".

P7 adds, "*The sanctions all depend upon the level of or the severity of the breach. So it depends on it. In the Public Sector, we have categories of whether it is a serious offence or a major offence. So if it falls within major offence, the applicable sanctions are there*".

- Compliance Monitoring

For compliance monitoring, the views of respondents was assessed into general and senior management roles.

Under general compliance monitoring, respondents were of the opinion that some factors such as human, technical/system monitoring, data monitoring, financial availability and personnel enforcement, among others, affect the organisation's compliance.

Regarding the human-centred factors and approaches, respondents noted that they are vital in ensuring compliance monitoring for ISP enforcement. For example, a respondent, P1, states, "*If you are doing a bad thing, someone will report. If you are not to go into a certain room or this machine, if you defy it, your own people will report you to your head of the department*".

Some respondents also believe that the managers are supposed to ensure that employees under them are aware and comply with the organisation's ISP. For instance, respondent P7 states, "*It is the managers that make sure that their staff comply. If the managers also do not do their work, Internal Auditors through compliance audit reveal and make sure that staff comply with the relevant security arrangements governing their areas*".

Another factor that some respondents identified as part of the human factors is employees' reservations about such Policy provisions and how they affect ISP compliance. This is because, as humans, employees naturally have reservations or concerns about policy compliance, especially when it involves personal data. When such people are involved in the development process, they are likely to frustrate the effective development process. For instance, P5 states: "*With the development aspects, some of the staff who must be involved if you want the policy to be successful, of course, will be brought in. But because certain aspects they might see as inconvenient to them and their day-to-day activities within your* *authority may invent reasons why they think policies should not be drafted in such a manner. That is the only drawback that I can see*".

Some management members believe that detective security measures using technical approaches help to monitor and detect non-compliance to the organisation's ISP and as a result act as compliance enforcement. On this, for instance, respondents, P4 and P9 state the following:

- *P4: We have systems support for monitoring compliance. And of course, monitoring can also be automated in various ways where, for instance, if you need to do a review by, say, this date and it is not done, the system flags it, and the person that is responsible is also flagged. And, of course, when that is done, it also goes a long way in ensuring that people live up to expectations because the system then becomes objective and not subjective. When you don't do it, the system exposes you and then you become liable to whatever punishment that may be applicable made. So these are the various ways I think the system can be used to monitor the implementation of these policies.*
- *P9: We know that we have to find systems. We, as the technology department, have to find an innovative approach to supervise. We don't need to leave it alone to the unit heads. We, as we sit here, should have tools and software to monitor in order to be able to know that in this department, somebody's using, say, an address that is not acceptable. So we have to monitor from the backend mostly. That's what I'm anticipating. And we are working on that. There's some tools too which could be used on them.*

Some respondents also believe that the recruitment or appointment of enforcement personnel and administrators in the organisation would ensure compliance monitoring and ISP enforcement. P7 for instance, asserts, "*Every unit should have its monitoring officers. The head himself is a monitor, and the head too should have supervisors who would also be helping him or her so far as monitoring is concerned*".

P7 further highlights that the internal auditors also can help in compliance enforcement by stating that, "*Apart from that too, like I said, internal audits, we also monitor officers. And our role is to make sure that the provisions within the security policy is complied with. So it's like we just take the checklist and use that checklist to do our compliance audit*".

Other management members also believe that using administrative, bureaucratic and regulatory approaches to enhance compliance monitoring and ISP enforcement by using standard operating procedures and automated compliance monitoring is critical to ensure effective compliance monitoring. A respondent P6 indicates, “*The monitoring can be effective through constant review of operations. So it should be through various SOPs (Standard Operating Procedures) that would determine how these things are done and at what intervals. It is something that is standard with various information security systems where we have standard operating manuals and standard operating procedures where constant reviews are done to ensure that what has to be done is being done. And what is not being done is addressed within policy. Through such appraisal mechanisms, one can monitor, and it can also be done at various levels from the top all the way down, where we have supervisory oversight at the various levels to ensure that everybody at their level is doing what he needs to do so monitoring can be done”.*

- Senior Management Role

Respondents indicate varied roles for the senior management in monitoring compliance. These include administrative and departmental Enforcement coordination, as detailed below:

First, respondents believe that it is the responsibility of senior management to ensure compliance enforcement. P4 expressed the view by stating, “*Monitoring systems. So I.T head also ensure that he checks on the CCTV and gets the report as to what's happened during the day, if there is a breach and all of that*”.

In addition, some management members believe that senior management should set good examples as leaders to attract other employees working under them. An example of such views is where P1 states: “*The senior management must themselves make sure that they do what they ought to do and stop what they ought not to do, because usually if you want to monitor, you yourself have to be clean*”.

P1 further adds, “T*hey by themselves have to prove that. If you are not able to comply with what you have put in place really, it doesn't exhibit a good way of monitoring breaches of the system*”, and P5 states that “*By themselves and their conducts also must behave and organise the department in such a way that conforms with the information security policy*”.

P8 also adds, "*Compliance can best be monitored when powers are given to the heads of departments and units to see their compliance. So when they all know their roles that they have to play in the policy, they make sure that it is carried out*".

The respondents also believe that senior management is expected to provide support to staff in terms of compliance as well as provide reports at their management meetings. P9, for example, states, "*The senior management must provide the resources, provide support*".

The respondents also highlighted that the senior management role in the enforcement process includes some key administrative responsibilities. For instance, as noted under the implementation role, the respondents indicate that the head of finance for instance, is to provide funding for the enforcement process, and the IT department provides technical support and protects the system. The procurement department also ensures that the organisation gets the best system possible.

- Compliance Status

The respondents were divided on the compliance status of the NIA ISP. While some respondents believe that there was a policy with no compliance, others believe that there was compliance but with some identified breaches. Those who say that there was no compliance enforcement included P9, and P9 stated "*For now, compliance is No. It is less than 20%*".

Other respondents note that it is difficult to state whether compliance with the policy exists, as there is some lack of clarity regarding what the policy is because of the status of the policy. P2 and P6 for instance state:

- *P2: And that's very difficult because with the kind of environment, there's no compliance. You can't have compliance.*
- *P6: Well, I am not quite sure if the arrangements are there in terms of compliance because constantly, I did not think any such policy was ever made available to staff. There has been attempts in the past to do enforce one that borders on Access control, Communication items like pen drives, personal laptops, restricted access to certain parts of the building and others. But over time, those were relaxed and were not enforced.*

For those that believe that there was compliance enforcement to some extent, they included P4 and P5 and commented as below:

- *P4: In my time, we didn't have many cases of breach. We did not have many cases of breach.*
- *P5: So to some extent, well, not a full-blown security policy was enforced, but just a little bit of "you can't have phones in this area" among others had been spelt out to the staff but not fully enforced as every now and then you could find people sitting comfortably within the server room area, systems administration area where they know they're not even supposed to have their personal phones, but then they do have them somehow. So it wasn't fully in force but there was a policy.*

In addition to the above, some respondents also believe there was less compliance enforcement due to conflict of interest arising from the attitudes and behaviours of the other institutional representatives on the organisation's Board of Governors. For instance, a respondent, P4, states, "*NHIA is on my [the NIA Board of Governors] board. Immigration went ahead, and immigration is on my board. SSNIT went ahead and did it; SSNIT is on my board. So, who can control all these other legally identified user agencies to make sure that we impose sanctions for breaches? Nobody can do that because they are the ones doing it. And so it becomes a bit difficult*".

Some respondents also believe that compliance enforcement was effective and successful. P5, for instance, states, "*The little that was pushed down, some people resisted, but the majority of the people were on board and played key roles to ensure it was successful*".

P4 adds, "*So I could say that, yes, in my time, we did our best to ensure that data was protected*".

H. ISP Evolution:

The ISP Evolution process discusses the challenges, participants, senior management roles and effectiveness of making amendments to the organisation's ISP. In general terms, the respondents believe key evolution challenges include organisational leadership, institutional and governance structure, and expertise support. On the evolution effectiveness, the respondents identified employees' knowledge and understanding of the policy and employee motivation as critical factors affecting the ISP evolution process. They further indicate that certain review aspects require internal and external stakeholders' involvement. For example, some respondents suggested that certain amendments to the policy should require the involvement of expertise as well as have legal backing from the national parliament of Ghana. A detailed discussion on the challenges, participants involved in the evolution process, senior management roles and the effectiveness of the amendment process are presented in the subsequent sections below:

- Challenges

Some respondents believe that changes in organisational leadership negatively impact the organisational amendment process. They believe that these changes do not allow the leaders the opportunity to complete some of the proposed reviews. For instance, respondents P5, and P7 state the following:

- *P5: I think there's a new leadership in place now. We actually did the work. And it didn't get a chance to go back to the board until we left.*
- *P7: The committee, they do not meet to do their regular review of these various controls; that's another factor. Earlier on, I even told you that sometimes, Internal Audit wrote about this Security policy, and this is the reservation that we raised, and this is outstanding.*

In addition, some respondents added that the willingness of the new leadership to adopt and continue the amendment process and get it approved was absent, hence a challenge to the review process. For instance, one respondent, P7, highlights, "*The committee, they do not meet to be doing their regular review of this various control, that's another factor. Earlier on, I even told you that sometime, Internal Audit wrote about this Security policy, and this is the reservation that we raised and this is outstanding*".

Some respondents also identified that institutional and governance structure is a critical challenge in the organisation's policy amendment process. They believe that the process or the structures required for the evolution process are either non-existent or cumbersome and time-consuming. A respondent, P2, for instance, sums this up by stating, "*It [the amendment process challenge] is the governance. The structures [referring to the policy provisions for reviewing the ISP] are not there*". The respondent, however, explains that such a process would generally have to include the involvement of external stakeholders like the sector ministry and the parliament of Ghana, among others, and these require a lot of time due to the workloads and busy schedules of personnel at the ministry or the parliament of Ghana.

A respondents posits, “*The review can be done through the parliament. We have to have a legal backing. You can't just get up and change certain things. So, the parliamentary aspect is very critical. We have to get it into the parliamentary service so that they pass it through the normal procedure to have it as a bill and then L.I (Legislative Instrument) or whatever you can call it. That's critical*”.

Finally, other respondents believe that a key challenge to the evolution process is that there is a need for specialist support to assist in the review process. They believe the expert needs to study the internal departmental processes to help the ISP review process. For instance, respondent P8 states, “*The people to be able to do that [referring to the evolution process] will have to come here and do a study and work through the different departments concerned. They must know the processes and approaches concerned*”.

- Effectiveness

Some respondents indicate that the NIA management regularly updates their policy to make it more effective. For instance, a respondent, P3, asserts, "*The amendment [of the NIA ISP] was done by management, and this was back then*”.

On the evolution approach, some respondents indicate that the amendment was done using the top-bottom approach involving management, the Board of Governors and some government officials to ensure effectiveness. A respondent, P6, for instance, highlights this by saying, “*The evolution will normally take the form of a top-bottom approach where a minister or the board is given a document to review or consider. When it is considered, it is then sent out to the management. Management further adds something to it. Management is expected to sell to both the internal and external stakeholders and if there is any other statutory requirements to ensure that the policy that is formulated meets every legal requirement then that also will take place. So in short, a public policy such as that of NIA where the process are clear, it is not like somebody's policy document. The document goes to the I.T department, it is reviewed by every department because everybody's role impacts on it and it is taken to the Board. The Board will look at it and if there are any contributions to it, it does. It comes back to the management, and then management owns the process and takes it through all the various stakeholder engagements and the approval processes. That is what I think is usually the case*”.

Some respondents also believe that the organisation’s executive secretary forms a committee to carry out the evolution process and submit it for approval. A respondent, P7, indicates, “*I think the Executive Secretary formed a committee to look at it. When they finished, they used the same process to get approval. Yes. Nobody can just fix it unless it does go through some approval process*”. P9 asserts, “*They [referring to the management members of NIA] will work with the team, the team that management has set up. And on who will be involved, I cannot say it because I'm not chief executive. I know definitely the technology unit will be represented and then Operation Unit will be represented*”.

Finally, some respondents also believe that the organisation outsources it to other organisations for the effectiveness of the ISP amendment process. For instance, P9 states, “*We are looking at writing to the authority [referring to the Board of Governors and the Government representatives for approval] to outsource the development [respondent believes that an expert organisation should revise and develop better and update policy] of proper and usable documents for that*”.

- Participants

As with the development process, the respondents indicate that internal and external stakeholders are involved as participants in the policy amendment process.

Regarding the internal stakeholders, the respondents mentioned key internal stakeholders such as the head of Technology and Biometrics, the head of Administration, the chief executive (Executive Secretary), the head of Finance and the head of Legal could review the policy. For instance, a respondent, P1, stated, “*I expect technology, administration, and you know, there is a legal aspect of this, so we need that lawyers, the head of legal, and then we need the finance people*”.

In addition, P2 and P9 respectfully added, “*You need first the IT people, it department, the chief executive, who is the supervising entity and then any other management member like the Legal department, because there are legalities in everything, the private partner*” and “*I know the technology unit will be represented and then Operation Unit will be represented*” respectively.

Further to the above, other respondents highlighted the need to involve everybody in the review process. They believe the amendment process is an organisation-wide process and must include everybody. For instance, P6 states, "*Internal stakeholders are as important as* *external ones. So one may expect that every person in the organisation will know about the mandate of NIA, will appreciate why he is there (in the organisation), and then every internal stakeholder will also be oriented towards knowing that they are employed there for the reason that whatever role they play impacts negatively or positively on what NIA does. So internal stakeholders are as crucial as those that are coming outside the walls of NIA*". The respondent further adds, "*Everybody because it is something that is for the organisation. So, in situations like this, when you do not involve everybody and by the state and by involvement, I mean getting everybody's input as much as possible for the policies to be finalised. So everybody is involved. Of course, the senior management members will be the drivers, but everybody in the organisation, as much as possible, should be made to be a contributor to the policy on their own small way*".

P8 adds, "*We should involve everybody because after a policy is developed, it moves into its implementation stage and then compliance. So if you are going to implement something and you force compliance, the very people that you expect to work with the policy need to be in the known. They need to understand why there is a need for this policy, what the benefits are and what role they're also supposed to play. So that is why, even if we want to amend what we have, times have changed, so we still need to go back to the basis and start from there*".

Regarding external stakeholders' involvement, some respondents indicate a need to involve experts and other external stakeholders in the evolution process. A respondent, P2, states, "*You must have people with expertise. And when there is a stakeholder consultation, the contributions will come to fine-tune it*".

In addition, some respondents indicate that the review process can be done by consulting similar external policies to guide the NIA ISP evolution process. For instance, a respondent, P5, states, "*Management made us add more to it; it went to the board. The board pointed to an institution outside the country, Malaysia and their policy for us to be guided by that*".

Finally, some respondents believe that the involvement of either internal or external stakeholders in the ISP amendment process depends on the nature of the gaps in the policy or the sections of the policy that need amendment. On this, respondent P7, for instance, highlights that "*I think it will depend upon where the gaps or where the need was. Security Policy covers various sections within the authority. So where the amendments are supposed to be made or take place, those unit heads of those particular units have to be part of the other relevant heads like Internal Audit, Head of Technology and Biometric, Operations, and*

Finance. These people should be involved. Yes. So, the key people here is those units where the amendment has to take place. Where the gaps call for the need to be amended. For them, we can't exclude them"

- Senior Management Roles

Respondents highlight the various senior management roles such as education, employee participation and making policy inputs and approval regarding the amendment process. Respondents also indicated that the senior management perform other key roles such as motivating employees' participation in the amendment process, investigating policy gaps, and seeking approvals for updated policy as discussed below:

First, on the education and policy review drafting, the respondents indicate that the senior management educate employees on the amendment process and they are involved in drafting the reviewed policy. On this, one respondent, P1, states, "*They play a major part in the amendment processes in terms of education and drafting of the policy*".

Regarding the making of policy inputs, P2, for instance, explains that the senior management, especially those who have experience working with the organisation, makes input to the review process and states, "*It is our input. Because for those who have worked here for long understand the system. No matter which area you sit, there's a global understanding. So you need the collective contribution from senior management as a commitment to mother Ghana because it's not for one person*".

Additionally respondents believe that the senior management should motivate compliance during the policy amendment process. On this, one respondent, P5, for instance, notes that "*Senior management have an additional role and responsibility to ensure that apart from they themselves conducting themselves in that manner, that people who can have them also are encourage and impressed upon to also conduct themselves in a manner that will not compromise on security of informatio*n".

Some respondents also indicate that the senior management investigates policy gaps and seek approval for the reviewed policy. For instance, a respondent, P7, suggests, "*Management can take a decision, and a committee may be formed to look into it and come out with various controls to address the gaps. When that is finished, and if management approves it, it will go to the top. Top management is the Governing board to give their final approval before we can implement it*". The respondent adds, "*I think the Executive Secretary* *will maybe form a committee to look at it. When they finished, they will use the same process to get approval. Yes. Nobody can just fix it unless it does go through some approval process*".

Regarding senior management role of driving the amendment process and ensuring departmental participation, respondent P8 notes, "*The senior management have to drive the process [the amendment process] because they are the heads of the units and the departments. So, if anything, it has to go through them, and they have to take the responsibility of ensuring that everybody's involved in the process and their contributions are well considered and well documented. So they have to actually drive the process*".

P9 adds, "*What I know is that the idea of having this amended was originated from my desk and then the teams were set up supervised by my desk to work on it. We have worked on it further, not finalised in this as I can say as to my expectation but it's something workable. It is something we can work with it when we improve on it*"

Respondents also assert that the senior management must provide the needed leadership and further supervise the amendment process. On this, a respondent, P9, states, "*Senior management will set up a team to supervise or manage it [amendment process] from the entire organisation. I mean, they will pick people from different risks-prone areas to be part of that*".

Respondents further highlighted that the senior management is to provide an updated policy that meets best practices. A respondent, P6, notes, "*They have to be constantly helping the authority to, first of all, have a policy that is made from best practices elsewhere. They also have the role of ensuring that the policy receives constant update if required"*.

Finally, some respondents also believe that the senior management role in the amendment process involves addressing identified policy gaps. Respondent, P7 states, "*I think it will be a management issue. So, the amendments can only come on if people, maybe some heads, realise that the policy needs to be changed or certain changes need to be made to address certain shortfalls or certain gaps. So they come out with those reasons. I mean, the need for those amendments to management*".

5.6 Discussion

This section aims to provide clarity on each aspect of the research work through a discussion for each of the three categories relative to the findings of this study and literature as detailed below:

5.6.1 IS Effectiveness

The responses of the participants indicate that the term "information security effectiveness" encompasses both human and technical activities aimed at protecting or enhancing the security of data, systems, hardware, and networks within an EIS organisation. This involves the participation of either internal or external stakeholders of the organisation or both. This aligns with Raggad (2010), who advocates for a multi-faceted approach to IS that integrates technical, operational, and managerial controls.

On the technical side, participants emphasised the importance of robust network security and encryption protocols to prevent unauthorised access and data breaches. This reflects the findings of Bulgurcu et al. (2010), who argue that technical safeguards are foundational to IS effectiveness, particularly when complemented by strong policy enforcement.

Equally important are the human factors. Participants highlighted the role of personnel in maintaining IS, particularly through adherence to security policies and fostering a culture of awareness. This is consistent with Jai-Yeol (2011), who notes that human error—whether intentional or accidental—can significantly undermine IS. Therefore, cultivating a security-conscious workforce is essential.

Stakeholder involvement was also identified as a critical factor. Participants noted that both internal (e.g., employees, management, board members) and external stakeholders (e.g., user agencies, private partners) contribute to IS effectiveness. This collaborative approach is supported by Raggad (2010), who emphasises the need for cross-functional engagement in IS governance.

Training and education emerged as recurring themes. Participants stressed the importance of continuous orientation and sensitisation programs to enhance staff understanding and commitment to IS practices. This aligns with Bulgurcu et al. (2010), who found that awareness campaigns and education significantly improve policy compliance and overall IS posture.

Finally, the importance of policy compliance and regular review was underscored. Participants advocated for involving technical experts in policy development to ensure relevance and robustness. This echoes the recommendations of Jai-Yeol (2011), who emphasises the dynamic nature of IS threats and the need for adaptive policy frameworks.

5.6.2 ISM

The data analysis underscores the respondents' consensus on the importance of prioritising IS management within EIS organisations. They emphasise the necessity of ensuring the robustness of systems and data through legal, administrative, human, and technical security measures to address concerns about personal data protection. This aligns with existing literature such as the World Economic Forum (2018), which suggests that these mechanisms help ensure and protect the choice, trust, and rights of individuals whose personal data is captured.

Raggad (2010) highlights issues related to the privacy, trustworthiness, and security of data collected, stored, and managed by organisations. These concerns are particularly crucial in identity management environments to prevent identity theft and other compromises (Raggad, 2010). The NIA recognises the importance of ISM and has made efforts to achieve international recognition through ISO certifications, demonstrating a commitment to protecting data

However, ambiguity remains regarding responsibility for ISM. While some participants pointed to the Technology and Biometric department, others cited various departments or the Executive Secretary. This lack of clarity can hinder accountability and responsiveness. Literature strongly supports the view that ISM is a shared responsibility across the organisation (Von Solms & Von Solms, 2004; ISO/IEC 27001). Assigning sole responsibility to a single department, such as IT, is insufficient. Instead, a coordinated governance structure involving all relevant stakeholders is essential for effective ISM.

5.6.3 Information Security Policies (ISP)

The discussion on ISPs is sub-categorised based on the following themes:

ISP Importance: Information security can be successful when organisations invest in both technical and socio-organisational resources to protect data and systems. Ensuring information security has become a top managerial priority in many organisations (Brancheau et al., 1996; Lohmeyer et al., 2002; Ransbotham & Mitra, 2009). This focus has led organisations to prioritise the formulation, review, and implementation of ISPs. ISPs guide employees in maintaining information security while using information systems for their organisational roles (Whitman et al., 2001). Some organisations have shifted their focus towards individual and organisational perspectives, recognising employees' compliance with ISPs as a critical socio-organisational resource (Boss & Kirsch, 2007; Siponen et al., 2007).

Research indicates that employees' behaviour can have both positive and negative effects on safeguarding information and technology resources (Bulgurcu et al., 2010). Bulgurcu et al. (2010) note that "Employees can help organisations safeguard information and technology resources by performing beneficial acts." Employees should avoid actions that compromise data security, networks, systems, or organisational resources.

The research data from this study highlights several other benefits of ISPs for the organisation, the government, and the citizenry. Respondents believe that ISPs allow the government to derive economic, political, and social benefits from the EIS. This aligns with Handforth and Matthew's (2019) findings, which show the economic, social, and political benefits of such systems. Literature also indicates that these systems have transformed the social, political, and economic lives of people (Nicoletta & Andrea, 2002; Gukurume & Mahiya, 2020).

Further to the above, the study notes that ISPs enable governments to provide enhanced services to citizens securely and facilitate safe data sharing among government institutions. For organisations, ISPs ensure data and system security by holding employees accountable and preventing data compromise, identity theft, and data loss. ISPs also help build trust among citizens, encouraging them to volunteer their data to the organisation and guide the organisation in performing its core mandate.

For citizens, ISPs help them access essential services such as travel, healthcare, and voting. ISPs also protect citizens from cybercrimes and other fraudulent activities.

ISP Status: Compliance with organisational ISPs is essential for successful executive functioning (Vardi & Weitz, 2004). EIS organisations must be aware of their ISP status for proper management. The ISP status informs management whether there is an effective policy in place and guides decisions on handling specific security issues by instructing employees on how to interact with the organisation's information and technology resources (Whitman, 2008). In the case of the NIA, despite varied opinions on the ISP status, most management members believe there is an ISP in place. However, the organisation needs to strategise to either review its policy or develop a new ISP and ensure it is formally approved to provide effective organisational governance.

ISP Awareness: The analysis of participants' ISP awareness aligns with existing literature. Staff awareness of the organisation's ISP is crucial for ensuring data and system security.

Sipponen and Vance (2010) for instance, have shown that staff violations of security policies often occur due to negligence or ignorance of ISP provisions.

EIS organisations should therefore have an ISP that addresses the need for staff awareness and compliance, as employees do not want to become ‘technical experts’.

ISP Content: The analysis of ISP content aligns with findings by authors such as Von Solms (2004), Tryfonas et al. (2001), Canavan (2003), and Raggad (2010). Von Solms & Von Solms (2004) emphasised that information security (IS) is multi-dimensional, requiring organisations to ensure the security of their information assets and environment. According to Wood (1995), information security deals with “the physical security of buildings, fire protection, software and hardware, personnel policies, and financial audit and control”.

Raggad (2010) suggested that organisations like the EIS must employ multi-faceted strategies, including ISPs, that incorporate technical, operational, and managerial controls to address critical concerns about data protection and security. These strategies ensure the confidentiality, integrity, and availability of information. Tryfonas et al. (2001) and Canavan (2003) also noted that an ISP is a set of rules or requirements related to information security, enacted by an organisation to protect the confidentiality, integrity, and availability of information and other valuable resources from security incidents.

In addition, some respondents' views indicate the need to focus on individuals, processes, and technology, as they are all needed to achieve adequate security. The respondents explain that such things facilitate the enactment and existence of a well-developed and approved ISP.

Further to the above, the need for multi-faceted approaches in developing EIS ISPs is evident, encompassing technical, operational, and managerial aspects. The respondents emphasised that a well-developed and approved ISP should be known to all staff and enforced using an effective reward and punishment approach. This aligns with Lewis and Baker (2013), who indicated that non-compliance with an organisation’s ISP can result in compromised data and systems, decreased organisational outcomes, and loss of interpretation.

ISP Development Process: ISPs are crucial for information systems security as they provide the blueprints for an overall security programme and create a platform to implement secure practices within an organisation (Von Solms & Von Solms, 2004). Researchers have identified that a well-developed ISP positively affects compliance with an organisation’s ISP (Siponen et al., 2007).

Flowerday and Tuyikeze (2016) noted that the important mechanism for protecting organisations’ assets includes how organisations formulate and implement their ISP. Whitman et al. (2001) added that organisations generally develop ISPs to guide employees in ensuring information security while performing their jobs using information systems. The development process of an ISP should therefore consider the processes to be used, the participants involved, potential challenges, the role of senior management, and approaches to ensure the policy’s effectiveness for adequate employee adherence.

This is particularly important for EIS organisations, as previous studies have highlighted the need for general effectiveness, security planning, and risk management. For instance, Kankanhalli et al. (2003), Straub (1990), and Woon and Kankanhalli (2003) addressed IS security effectiveness, while Soo Hoo (2000), and Straub and Welke (1998) focused on security planning and risk management. Doherty and Fulford (2006) and Siponen and Iivari (2006) also indicated that the ISP development process should address issues related to the design, development, and alignment of ISPs.

Additionally, the responses from the data highlight the importance of considering both internal and external stakeholders’ influence in the development process of the EIS ISP. Factors identified include participants involved in policy development, challenges identified by stakeholders, the effectiveness of the ISP development process, and senior management roles. This aligns with Knapp et al. (2009), who suggested that several internal and external influences affect an organisation’s ISP development. Internal influences include senior management support, business objectives, organisational culture, technology architecture, and internal threats. External influences include the economic sector, technology advances, industry standards, legal and regulatory requirements, and external threats.

Given these factors, it is crucial to ensure that staff are aware of the need to participate in the organisation’s ISP development process. Staff should be educated about the ISP development process, the impact of their actions, and senior management’s role in ensuring general information security. When the right participants are involved and well-informed, there will be minimal challenges during the ISP implementation phase.

ISP Enforcement: Research highlights that ISP enforcement significantly influence the behaviours of employees in protecting their systems and data. Stanton et al. (2005) argues that merely having an ISP is insufficient for ensuring information security; employees' adherence to these policies is crucial for successful organisational functioning (Vardi and Weitz 2004). Knapp et al. (2009) emphasise that ongoing policy enforcement helps management integrate these policies into formal procedures, keeping employees in check. Raggad (2010) further asserts that a good information security policy should be "easy to revise, communicate, and enforce". EIS organisations must take steps to address issues that relate to compliance by enforcing their ISPs. This is because, generally, research has focused on the noncompliant behaviours of employees (Willison and Warkentin, 2013) and the way those employees "pose serious threats to their organisations" (Belanger et al., 2017).

While some organisations, to ensure compliance, resort to using technological means to enforce some or part of their information security policies, the attitudes of some staff pose a challenge. Alzahrani (2018) emphasises the essence of implementing the organisation's ISPs by indicating that human behaviour also positively reinforces compliance. As such, organisations must encourage their employees to comply with their ISPs. Bulgurcu et al. (2010) also highlight that organisations have recognised that employees who adhere to the information security rules and regulations play an integral role by being significant assets in reducing information security risks and helping to leverage the organisation's human capital.

The above situates with the analysis of data in our research. The data from this study indicates that provisions to motivate or reward staff and sanction non-compliance should be part of the policy.

Again, Compliance monitoring should involve managerial, technical, legal, and socio-human approaches and Senior management should act as pacesetters, monitor subordinates, communicate effectively, and educate staff on their roles

Overall, the views of the respondents highlight the critical issues related to ISP enforcement within digitised identity systems. Addressing these concerns through comprehensive enforcement strategies, motivation, and effective monitoring can enhance the security and integrity of the Ghanaian National Identity System. The views also highlight the urgent need to ensure there is clarity regarding ISP compliance in EIS institutions to protect the data and the system.

ISP Evolution: The involvement of humans in the security of IS systems is critical because they manage the invaluable assets to organisations, which are information (Belanger et al., 2017). While protecting information is essential, regularly updating the EIS organisation's ISP is equally important. According to Nurse et al. (2014), changes to security policy (e.g., forced password changes, required password strength, and automatic security updates) could become the catalyst for negative attitudes and undesired behaviours in an organisational environment. This underscores the need for constant or regular evolution of ISPs to adapt to changing times.

To effectively amend the ISP, it is vital first to assess the effectiveness of the existing ISP and identify any issues. Once these problems are identified, decisions can be made regarding the participants involved in the evolution, how to address the challenges and the roles senior management should play in the amendment process. The current study highlights some unique challenges faced by public service or government-controlled EIS ISPs, including rigid public service legal/regulatory processes, organisational leadership changes, and the willingness of EIS management to carry out ISP evolution.

The research highlights varied opinions on the general effectiveness of the ISP. Some respondents believe that evolutions are conducted, while others do not. Opinions also differed on the review approach, with some citing a top-down approach, others mentioning a committee formed by the Executive Secretary, and some believing the organisation outsources the review to experts. This indicates an urgent need for management to educate employees and create awareness to ensure better effectiveness in the evolutionary process. Respondents highlighted various approaches to involving participants in ISP amendments. Some believe only crucial management members should be involved, while others advocate for the inclusion of all internal stakeholders, including management and staff. Consulting external EIS ISPs during the amendment process and involving both institutional and non-institutional external stakeholders were also suggested. Participant involvement should be based on identified gaps in the existing EIS ISP. The organisation needs to clarify its approach to studying and amending its ISP.

Regarding the Senior Management Role in the evolution process, respondents emphasised several roles for senior management in the evolution process, which align with literature recommendations. These roles include education and policy review drafting, ensuring employee participation and action during the evolution process, providing updated organisational policies, investigating policy gaps and seeking approvals for amended policies, driving the amendment process, ensuring departmental participation, and supervising the policy review process. While these suggestions are valid, the organisation needs to clarify its approach to studying and amending its ISP.

5.7 Concluding Remarks

The chapter discussed the aims and objectives of the second study that focused on management's views about the NIA's IS effectiveness, IS management, and ISP. It also justified the qualitative method used for the study, the participants and procedures used for the research work, the results of the study, and the analysis of the research conducted.

Generally, the study highlights management's perceptions of the NIA ISP and its formulation, enactment, and development processes. It also analyses their responses to their ISP regarding employees' involvement, compliance, and awareness. The research also assessed the effectiveness of the NIA ISP, its content, importance, enforcement, evolution processes and the status of the policy.

In terms of some observations from the data, we can say that the research work generally enforces the need for some essential considerations in developing an ISP for Electronic Identity Systems by recognising that both employee perception about ISP issues and real ISP issues are crucial to such EIS organisations and as such must be managed effectively. This can be done by formalising the development policy approach process and approving the policy in line with government regulatory guidelines in the country.

Regarding IS effectiveness, the research highlights a need to work on general IS issues and approaches that can improve the organisation's existing IS strategy. The study also indicates how public-private partnerships impact the IS effectiveness in the organisation.

Regarding IS Management, the study indicates that the involvement of experts, administrative strategies, the assurance of IS Awareness and Staff Training, and Access and Password Management can impact the organisation's general IS management.

On the ISP, the study shows that a positive attitude towards compliance, ISP awareness and training, and physical, human and technological security enhancement approaches must be adopted by EIS organisations. In addition, the study indicates the importance of involving internal and external stakeholders in the formulation, development, and implantation phases of the ISP.

The next chapter focuses on the study conducted on NIA External stakeholders' involvement, development, and implementation processes.

6 Study on External Stakeholders View (User Agencies)

The previous chapters (chapters 4 and 5) assessed the views and thoughts of the internal stakeholders about their involvement in the ISP development, implementation and evolution processes.

This chapter focuses on the user agencies' views and perceptions about their involvement in the NIA ISP development, implementation, and evolution processes. This was conducted by interviewing the respondents. These user agencies are considered the NIA's external stakeholders. To provide detailed insight into the findings, we begin with the study design section, then the participants and study procedures, followed by data analysis, the study results section, the discussion section and, finally, a concluding remark.

6.1 Study Design

In Chapter 3, we explained why we designed a semi-structured interview guide for the interviews. In this study, we used the semi-structured interview guide to elicit responses from identified external stakeholders of the NIA about their understanding, perceptions, knowledge, and involvement in the NIA ISP development and evolution process relative to compliance and enforcement.

More specifically, we posed questions to assess the user agencies' (both institutional and non-institutional) perception of the NIA ISP by interviewing them. The interviews also assessed the effectiveness, importance, and status of the NIA policy. This was part of our attempt to find answers to the following sub-research questions:

> **RQ1:** How effective are the NIA Information Security Policies in protecting its Identity Systems?
>
> **RQ2:** What are the NIA external stakeholders' views and thoughts about Information Security in Identity System Organisations?
>
> **RQ3:** To what extent are the NIA external stakeholders involved in the development, awareness creation, compliance, enforcement, and evolution processes of the Information Security Policies in Identity Systems?

6.2 Participants and Procedures

6.2.1 Participants

We targeted the NIA's institutional and non-institutional external stakeholder organisations for this study (see section 3.7). The institutional organisations were those that have formalised relationships with the NIA and have representation on the NIA Governing Board. Non-institutionalised organisations are those that rely on the NIA to provide services such as customer verification, authentication, and information sharing to citizens and residents but have no representation on the NIA Governing Board.

To this effect, we identified and invited 17 out of 20 identified external stakeholders. We invited the organisations based on a distribution formula. The distribution formula was developed primarily based on the number of external stakeholders whose operations demand some collaboration or reliance on the NIA. The excluded ones included Airtel Tigo (a telecom company) Zenith Bank and Ecobank. The exclusion was due to potential non-cooperation due to the managerial issues prevailing in the organisations at that time. For instance, Airtel Tigo was preparing to stop operating in Ghana while Zenith and Ecobank may need external approval from their corporate headquarters based outside Ghana. We then sent an invitation letter from the head of the Strathclyde CIS Department to the selected organisations' heads.

However, due to the time limitation and some institutions' non-interest in participation, we could interview thirteen (13) senior members of the identified organisations to elicit their responses as set out in the semi- structured interview guide to better understand the ISP processes from different organisations' perspectives (see details in appendix 9.6).

.

6.2.2 Study Procedures

As noted in Chapter 3 in the study procedure section, we obtained ethics approval from the Department of Computer and Information Science's Ethics Committee for the study. We also received approval from the organisations' heads, who nominated the right persons for us to engage with/ interview on behalf of the organisation (see details in Appendix 9.4).

As noted in the methodology chapter (chapter 3), the interview session was face-to-face, and each of the thirteen participants lasted a minimum of 45 minutes.

The interviews were conducted at the headquarters of each of the organisations in Accra. The interviews were conducted between 20/01/2022 and 20/03/2022. After the interviews, we transcribed the recorded audio with the "Temi" software into Microsoft Word and uploaded them into the NVIVO software for further analysis. Using the NVIVO software, we coded the responses into themes.

6.2.3 Pilot Study

Before the main study with the external organisations, we conducted a pilot study with seven PhD research students in our department. We then asked for their feedback, which was used to improve the study design for the primary data collection exercise. The feedback uncovered some minor issues about the structure of the questions. Others were on the identification of ambiguous questions and testing of the results. The problems identified were all corrected. Each of the participants for the pilot studies spent about 60 minutes.

6.3 Analysis

The study focused on thematic analysis resulting in themes and sub-themes under each category. As with Chapter 5, we also described each category's themes and sub-themes.

To synthesise the data further, we adopted the bottom-up approach to group similar and different codes together to make meanings from the data and answer the research questions as detailed in Chapter 3 (section 3.11.4).

After synthesising the data, we confirmed the research findings by verifying and validating the codes and themes to ensure they accurately represent each respondent.

6.4 Demographic Results

The results section is divided into two main groups: demographic results and non-demographic results.

With the demographic results, we analysed the personal data of respondents, such as their position, how long they have been in their position, and their primary responsibilities.

The table below details the participants' demographic data for the study:

Participant	Institution	Position	Years on Position
E1	Access Bank	Senior Member, Information Technology (IT) Infrastructure	5 years
E2	ADB	Senior Member, Chief Information Security Officer (CISO)	1.5years

Participant	Institution	Position	Years on Position
E3	Birth and Death	Senior Member, Information and Communication Technology (ICT), Projects, and Programmes	15years
E4	CAGD	Senior Member, IT Operations, and Infrastructure Management	5years
E5	GIS	Senior Member, Management Information System (MIS)	6years
E6	GPS	Senior Member, Cyber Crime and Digital Forensic	6years
E7	GRA	Senior Member, IT Transformation	2years
E8	GRA TIN	Senior Member, Taxpayer Identification Unit	3years
E9	NHIA	Senior Member, Business Systems, MIS	9years
E10	Passport	Senior Member, Passport	2years
E11	SSNIT	Senior Member, IT Application Development	1year
E12	Stanbic	Senior Member, CISO	8years
E13	Vodafone	Senior Member, Cyber Security Compliance Specialist	9years

Table 14: Demographic Distribution of Respondents

From Table 13 above, we note that all participants were senior serving management members with varied responsibilities. The participants' responsibilities were executive, administrative, and technical roles, and in terms of years in their positions, they ranged from one year to 15 years.

6.5 Non- Demographic Results

The non-demographic results were categorised under three main sections (see details in appendix 9.9b) for effective presentation, which included:

- Information Security Effectiveness (Effectiveness),
- Information Security Management (IS Management) and
- Information Security Policy (ISP)

6.5.1 Research Categories

The research analysis yielded 15 themes (2 for IS Effectiveness, 5 for ISM and 8 for ISP).

- Information Security Effectiveness (Effectiveness): The Effectiveness here refers to the participants’ concerns and beliefs within the IS context. Under this, we had two themes: General and Improvement.
- Information Security Management (IS Management): Under this, the ISM focused on respondents understanding and views about the security and management of both data and systems. The IS Management was categorised into five (5) themes: effectiveness, emphasis, Responsibilities, NIA Relationship and Senior Management Roles.
- Information Security Policy (ISP): The focus of the ISP is to understand the views and perceptions of respondents about the NIA’s ISP development, implementation and evolution processes. To do this, we categorised the ISP findings under eight (8) themes which included ISP Awareness, ISP Content, ISP Development Process, ISP Enforcement, ISP Evolution, ISP Importance, ISP Governance Effectiveness, and ISP Status.

Using the Treemap below, we highlighted the various components and relationships of the study categories, themes, sub-themes, and sub-topics. The Grey colour shows the themes and sub-themes that fall under the ISP category, the blue represents themes and sub-themes under IS Effectiveness, and the brown represents themes and sub-themes under IS Management. Interestingly, the data treemap shows that the ISP category is slightly more dominant in the research than the ISM management with the least of the three categories being the IS Effectiveness category, as shown below:

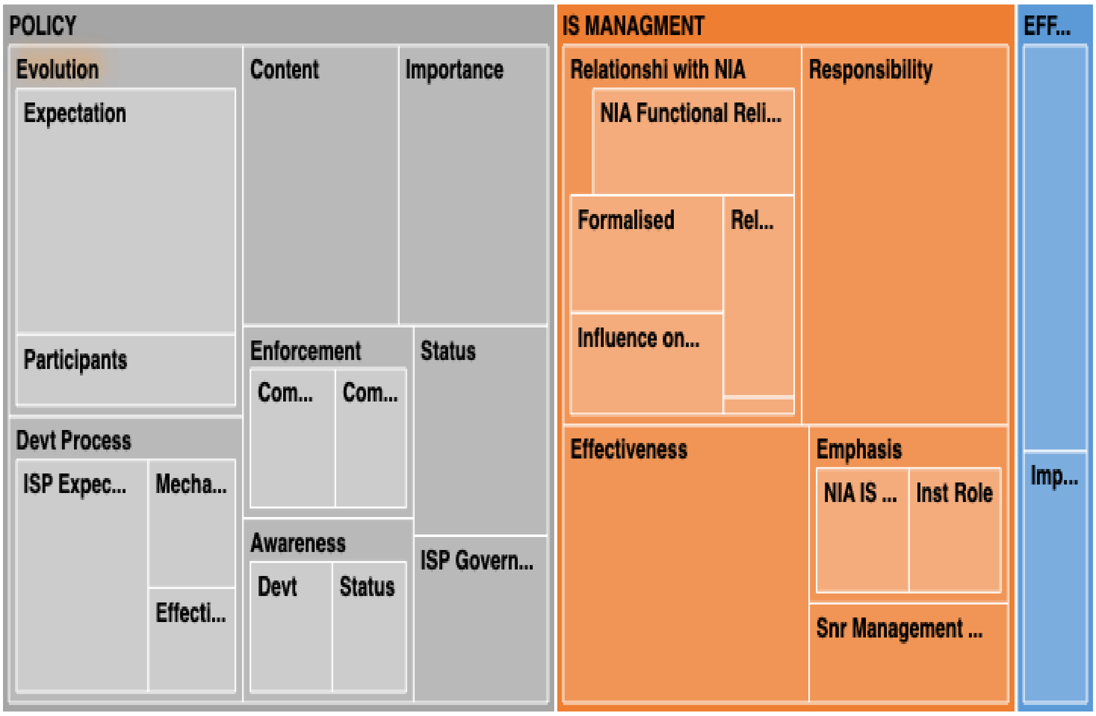


Figure 21: Treemap Showing components and relationships of categories, themes, sub-themes, and sub-topics

6.5.1.1 Information Security Effectiveness

General IS Effectiveness

On general Information security effectiveness, the respondents focused on Data compromise/ security issues, Data Access Control, regulatory control, collaboration and confidentiality of data.

On the data compromise, the respondents showed or expected that the NIA provides effective information security to secure the data and the system. E1, E3, E6, E9, E12 and E13 support that. Examples include the following:

E1: Of course, it should be effective. As I mentioned earlier, the kind of connection we even send via their environments should be through a secure channel, and then, the kind of security measures they're putting up for the country, I believe they've to be secure as well.

E6: All the necessary security must be put in place to ensure its security, from physical security to network security, to data security, software, and hardware, and every part of it must be protected.

E13: IS effectiveness is of high concern when protecting the data and systems of the organisations involved.

On Data Access Control, the respondents highlight that they expect to see that the necessary protocols for secured access by user agencies and the provision of restricted access levels for validation by each user agency are in place. On this, for instance, E3 states, "*Although the national ID system was built with many security concerns in mind, and now that they are open for validations, what protocols have they put in place? Are the security protocols put in place for other user agencies secured for them to log onto their platform to validate NIA cards? My issue of concern is: how many levels of access do they have? Is this direct access to the database, or there's a front end that searches the data to that front end for users to validate NIA cards*".

Regarding regulatory control, the respondents acknowledge the existence of laws to guide data management. A Respondent E3, for instance, cites the Data Protection Law as an example and states "*As we speak in Ghana, the Data Protection Law has spelt out in detail what kind of security is needed to be put in place when it comes to sharing information and when it comes to taking information on individuals*".

On collaboration, the respondents acknowledged that, the security effectiveness of the data and systems could be achieved when the internal and external stakeholders collaborate. For instance, on the internal, E4 states, "*It is secure in the sense that the owners play their role. The IT side also plays its role by ensuring that the systems run efficiently and that the controls the owners proffer are implemented and working well. These people ensure that the controls work. They come to audit from time to time"*.

E5 further adds that external expertise involvement can effectively identify foreigners who attempt to register by stating that, "*We would've wished that we could even play a participatory role in registering an applicant as a citizen of Ghana. This is because we have been trained to be able to identify faces, to be able to identify the faces of human beings and the characters to know that this particular person doesn't sound a Ghanaian or doesn't look like a Ghanaian, even though somebody cannot just look at your face and say that you're Ghana or not. But based on our training, I can look at this person and say that this person is Korean, Chinese, or Japanese based on our training and because we have worked with the people*".

Finally, on data confidentiality, respondents such as E8 and E11 acknowledged the importance of protecting individuals' data to protect their privacy. On this, for instance, E8 state "*Once you're collecting data on an individual, it's important that you are concerned with ensuring the information is confidentially kept as required".*

For E11, he explained that he expects the organisation to put in place measures to ensure data integrity and confidentiality and stated, "*I think one area of concern is the confidentiality of the information that they gather from individuals. I think they have to put in place measures, so that that information is confidential. And also the integrity of that system so that when I verify an account today, when I come back next year and I want to verify, I should still get the same feedback that I got last year so that there's nothing like somebody altering the content along the way"*.

IS Effectiveness Improvement

On improving information security effectiveness, the respondents highlighted effective data collection, data sharing, resource sharing, compliance enforcement, engagement/ participation of stakeholders, recruitment and training, and the need to improve security improvement as ways that IS effectiveness could be improved.

For effective data collection, respondent E3, for instance, acknowledges that improving IS effectiveness would "*guide and enhance the quality of data collection*" and argues that "*if I'm picking data on an individual from the lower level, and I'm well educated with this policy, every question I ask, I'll put the right questions to get the correct answer. So, you see that it'll filter through the system. Once I get that right, the national identification system lacks errors or minimises them*".

On data Sharing, the respondents suggested that there should be an improvement on data sharing to allow effective verification and authentication. For instance, E10 stated that the passport office can verify NIA information on their system, but the NIA cannot verify passport details sent to them by saying, "*They share with us, but we don't have the opportunity to share with them. And I don't think they have a link to the passport office where you can see the person's passport details when you click. The passport you accept is the basic requirement for them to get their card; you don't have it in your system so that when you key the passport number, you see the person's information. But when we click on our system, we see the NIA information here. So, they only share with us, but we don't have the means to share with them*".

On resource sharing, respondents acknowledged that there should be an improvement in resource sharing to improve IS effectiveness. E3, for instance, summed this up by stating, "*There are many prospects when it comes to improvement. I think that the NIA and my organisation have to go to some level of agreement to share resources because they complement each other. They can complement each other and also improve the mode of transmission, apply technology more, improve security, improve connectivity, and make sure integration processes are in place*".

On compliance enforcement, respondents believe that they expect clarity and adequate enforcement provisions to ensure effective IS enforcement. On this, E4 and E7 share their views as follows:

E4: My area will be the policy. Every policy has enforcement provisions, and then it has provisions for whether people should renege or not go according to it. But generally, in public service, people tend to frown on it when you come out with things like that. And they tend to sort of belittle the enforcement. I expect whatever policies come out will be straight to the point. And then, it will have a portion with whatever punishment should be meted out to the people so that it will be unambiguous. Anybody who takes it knows that if I should infringe on this provision, this is what should happen.

E7: It is extremely important that the NIA, as an organisation, is able to enforce its security policies, stay on top of the enforcement, and have periodic interventions to check to ensure that all the pillars that they have held their policies are in place and can control, and then execute interventions right afterwards if any of them do not hold.

Respondents also expect that engagement /participation could be improved to enhance IS effectiveness. Respondents further highlight that the external stakeholders' involvement significantly helps in decision-making and effective IS management. E5, E8, E9, E10, and E12 supported this assertion. For instance, some of the comments are as follows:

- *E8: We think there should be more engagement in decisions that will affect the Ghana card registration activities, which are being done especially in our offices and even in their own offices. This is because when someone wants to come and pay tax right now, and NIA activities are off, without the TIN, which is now the Ghana card number, how can the person not pay?*

- *E9: All parties involved must participate actively and champion it for it to be a Norm. We do our bit in our operations to get it stabilised. We all need national identification. We are working closely with NIA in doing N H I S membership and NIA or Ghana Card linkage and continue to collaborate actively in that effort.*
- *E10: There could be ways to devise ways of engaging with the state agencies and see how best they can approve and improve the general operations.*
- *E12: I think they should be transparent with stakeholders on how they are handling the information they are collecting, how the information is processed and how the information is being protected and largely, the stakeholders would believe and trust that they're doing the right thing. Also, there should be an avenue where stakeholders can provide feedback which they can incorporate into the evolution of their policy.*

Regarding recruitment and training needs, respondents acknowledged that they expect the NIA to enhance their IS's effectiveness through an effective recruitment process, security background and employee training on key issues such as the Citizenship Act, NIA Regulatory Laws, and Criminal Laws, among others. On this, for instance, E5 sums it up by stating, "*NIA should not limit it to only its staff because of the way they train their staff. Their staff should also have a background in security training. They should have a background in security training and know the importance of the data they collect for the state. And they should know the laws of the state. They should know the law that governs citizenship and not just any other person they recruit. They should send them to go through discipline training like security personnel goes through discipline training and know the laws. It makes them know that "this is the law of NIA; this is citizenship Act. These are the laws of immigration and then the Criminal Code. The person should have a fair idea of such laws to be able to sit and give the go-ahead that "this person is qualified per the registration act or by the laws*".

Finally, the respondents believe that ensuring enhanced security, information privacy and business continuity could improve IS effectiveness. E7, E10 and E11 supported this. For instance, they state as follows:

- E7: *Security is extremely important because security is actually what warrants and guarantees our business continuity. If we don't have effective security, we cannot effectively execute the mandates that we have as a government, or for that matter, the mandates that we have as revenue mobilisation officers*.

- *E10: What I do observe is that some other sectors are of the view that the NIA is somehow managed by a private person, and they wish it should have been managed by the government. Therefore, they conclude that in this regard, some improvement is needed from the government.*

6.5.1.2 Information Security Management

The IS management focused on external stakeholders' IS effectiveness, senior management role, IS responsibility, and relationship with the NIA, emphasising the external stakeholders' and NIA IS roles. From the study, the respondents highlighted that the role of senior management included providing administrative, organisational and technical resources to provide security to data and the system. The respondents also highlighted the provision of appropriate policies to ensure compliance by user agencies and their personnel for effective IS Management.

To better understand Information security management from the perspective of the external stakeholders, the following five themes from the data are discussed:

ISM Effectiveness

On the ISM effectiveness, the respondents highlighted key issues related to data security, network security, security controls, trust, and legal and regulatory requirements. Generally, the respondents believe that ISM is appropriate due to the nature and type of data that EIS organisations manage. The respondents also indicated that, when such provisions are in place to enhance the effective management of the NIS, it would help achieve the organisation's mandate.

On data security, for instance, E1 highlighted, "*Information security is, in fact, the order of the day. Your ability to manage and then secure your customer data goes a long way to affect your activities. For instance, if it's heard that customer details have been stolen via your bank or via your institution, you surely know as well that you may go down with it*".

E11 also adds, "*I think it should be something of major concern because they are dealing with information on Citizens. And so I think they should be concerned about information security so that they wont leak information to unauthorised person"*.

The respondents also explain that it is due to ensuring effective ISM that some institutions have considered it critical. For instance, E11 states, "*So it's something that we as bankers have taken very critically*".

Some respondents also highlight that an EIS organisation should consider ISM effectiveness as prime and protect their system and associated litigations. E5, for instance, believe that "*Information security bothers with the security of the data that they collect*".

E5 also posits, "*It* [information security] *should be a priority. It should be a priority to them because they are taking information of the whole country. And if you look at the Data Protection Act and there is a data breach, the individual or the group of individuals can sue them and they are an entity of the state so they can be sued and they can also sue. And for that matter, it is very important. It should be a priority to the NIA*".

Other respondents explain that an effective ISM could guide and improve data quality and minimise system errors. On this, E3 state, "*It'll guide and improve the quality of data collection. For instance, if I'm picking data on an individual from the lower level, and I'm well educated with this policy, every question I ask, I'll ask the right questions to get the right answer. So, you see that it'll filter through the system. Once I get that right, the national identification system is minimal or error-free*".

E1 and E9 also add that effective ISM helps organisations to have great data and protect individual information by stating, "*One [itemising it as number 1] is for you [referring to organisations] to have great data. Two [itemising it as number 2], To ensure that your data that you gathered is of quality. No interferences is also there. And then it is a duty for the NIA to protect the individual information as it relates to the national security*".

On Network security, E1 for instance, notes, ISM "*should be effective… the kind of connection we send via their environments should be through a secure channel*".

In terms of security controls, the respondents emphasised the need to ensure administrative, technical, and organisational controls to ensure adequate security. E2, E4, E5, E6 and E8 acknowledged this. For instance, E2 states, "*It's important that NIA put in place the minimum-security control through the use of administrative, technical, and organisational control or a combination of these so that threats posed to identity management are proactively prevented or detected in a timely fashion using technical identity and access management solutions. In worst-case scenarios, the right corrective mechanisms should be put in place for corrective controls, such as backups*".

Respondents also acknowledge trust and confidentiality issues that must be addressed to improve ISM effectiveness in EIS organisations. On this for instance, E2, E5, E8 and E12 agreed on it. Examples are as follows:

- *E5: All boils down to information security because if you have an untrusted person in your system and he plugs in something onto a network point, he can harm the security of your data.*
- *E8: Yes, it's appropriate because they're holding the data of all individuals, and there's a need to ensure that whatever information that they are collecting is confidentially done.*

On legal and regulatory requirements, some respondents highlighted that ISM effectiveness can be enhanced using regulated organisations. For instance, E4 asserts that the cybersecurity organisation in Ghana ensures that ISM is effective by regulating how EIS organisations manage personal data. The respondent explains, "*As an individual, I have to give information to the National Identification Authority. My date of birth and everything is with them and my fingerprints. So it is of high security that they take good care of it. But I think everything is regulated mainly by the cybersecurity organisation and the National Information Security Authority or information authority*".

ISM Emphasis

The ISM emphasis focused on information security status, the NIA IS role and the external organisation's IS role. The respondents acknowledged the roles that NIA and their organisations play and the effectiveness in ensuring ISM in their organisations.

On information security management status, respondents were of the view that it is of high concern, while some few indicate that the IS status is on an average basis.

Those that believe that it is high concern include E1, E4, E5, E6, E7, E8, E9, E10, E10, E11, E12 and E13 and justify their beliefs why it is appropriate. The comments ranged from the type and sensitivity of data stored. An example is where E7 states, "*It's very high and appropriate because every Ghanaian has his information living with NIA, so information security is extremely important. And I get it because of the awareness by the staff of how concerned senior management is about the security of the information in our hands. And so, it's been effective*".

E9 also adds, “*Having to have NIA as the prime entity in managing verifiable personnel identification, it is critical that security is a prime concern. We have to depend on NIA's reliability, as in the data, for us to continue with our operations. Its security is prime, and for us to offer the kind of services that we need for our members, we need to be assured that security is guaranteed on the prime data that we depend on to operate*”.

Those who believe it is moderate include E2 and E3. For instance, E2 states, “*On a scale of 0 to 5, the ISM is about at about level 2”.* E3 also adds, *“I think in terms of information security for the national ID, I would rate it medium as we speak now because there have been times that we've even heard leakage of national ID information by some private agency*”.

On the NIA IS role, respondents acknowledge the need for the NIA to provide adequate security to protect its computing environment and ensure information security. For instance, E1 asserts, "*I think security should be a concern to the NIA, judging from the fact that even how we connect to the environment should be via a secure environment*". E2 adds, “*One of the key foundations of information security is uniqueness and verification of identity*”.

In terms of the external institutions’ role in ensuring IS, respondents acknowledged it and highlighted that it is important to ensure data security and adherence to data management regulations. To achieve this, some institutions have subscribed to professional data management standards. For instance, E1 states, “*We've been certified ISMS, BCMs, and PCIDMS for the past three or four years. So, I believe for these four years, we've done pretty too well. Sure. We've not had any serious breaches in security, so I believe we're doing well*”.

E2 also supports the above by stating, “*Information Security is a major concern for banks and the general ecosystem. Legal authorities and regulators have passed security requirements to ensure the digital space is sanitised and adequately protected from cyber threats. These include ISO27001, PCIDSS and Data Protection Act, and Critical Infrastructure Directive*”.

Other respondents also acknowledged that as part of the external IS role, there should be stakeholder consultations to ensure effective collaboration. On this, E2, for instance, states, “*There are stakeholder consultations still ongoing among banks because of issues raised about the adequacy of current arrangements within the NIA infrastructure*”.

Some respondents highlight that external stakeholder institutions like theirs must prioritise ISM due to people's privacy and confidential concerns about the data they also process. E4, E8, E9 and E10 agreed on this. For instance, E9 underscored that “*For us, and the kind of data* *that we maintain, it borders on confidentiality, privacy, and all that, and we manage health data. It is critical that everybody has the confidence that their health data is protected, considering the Data Protection Act, which ensures that we conform to the Act and beyond*".

ISM Responsibilities

The ISM Responsibility analysed the responsibilities of respondents and where ISM responsibility lay within their organisations.

Respondents' Responsibility: The respondents believe the IS responsibilities reside with individuals heading specific management departments or units. They mentioned internal individuals or departments ranging from chief information security officers (CISO) to MIS heads. In particular terms, E1, E2, E3, E7, and E12 respondents opined that their organisational IS security lay with the Chief Information Security Officer. Examples of some of their responses are:

- *E1: Our organisation is structured such that we have an information security unit, which is managed by the CISO.*
- *E2: Primarily, it is the Chief Information Security Officer*
- *E7: We have a CISO (Chief Information Security Officer) process and a security person responsible for that.*
- *E12: That is the chief information security officer (CISO).*
- E5, E6, E8, E9 and E11 believe that the MIS or ICT departments or units were in charge of managing ISM in their organisations. Examples of their comments were as follows:
- *E5: Information security management is the responsibility of the head of the Management Information Systems department. He is responsible for managing the information the security of the service of GIS.*
- *E6: If we talk about information security, it's our ICT department. They are responsible for managing it because they are in charge of the infrastructure for the police.*

Some respondents also believe the responsibility lies with external national organisations, such as the Cyber Security Authority Unit and the National Security Secretariat. Such respondents, included E10 and E13 stated the following:

- *E10: It is the national security. They manage it. Then, we have well-trained officials from the Ministry of Foreign Affairs I.T. They protect, and then they work on our data.*
- *E13: The Cyber Security Unit is responsible.*

Primary Responsibilities: On the primary responsibilities, the respondents highlighted critical roles in ensuring adequate information security management in their organisations. The varied roles that they play include systems and IT management, information security management, policy governance management, technical support role, and compliance enforcement.

On systems security and IT management, for instance, E1, E3 and E12 agreed. An example of their responses is where E1 states, *"As the head of infrastructure, I ensure that our systems are up and running in terms of our network aspect by ensuring that we get as good as required from our internet service providers. We ensure that their services are very reliable since we actually rely on them to ensure that services are delivered to our customers*".

On information security management, E2, E4, and E8 affirmed this role. E2 for example, asserts that his responsibility includes driving information security strategy and implementation in the organisation by stating that he is in charge of "*Driving the Information Security Strategy and implementation whilst protecting the Bank from security threats and cyber-hacking"*.

On policy governance management responsibility, E5, E7, E9 and E13 align with that primary responsibility. E5 for example notes that he is responsible for policy formulation and managing IT information infrastructure, as well as ensuring effective supervision, coordination and monitoring of external projects. The respondent states, "*One of them is policy formulations. I have also been the one who manages the I.T infrastructure and the critical information infrastructure of the service; I supervise and monitor external projects and also review all in-house projects or in-house I.T Software that are being developed for the service as well as report to the head of MIS for management decisions to be taken*".

On the technical support role, E10, and E11 affirmed these responsibilities and explained that such roles included providing technical advice and managing in-house developed applications. E10 for instance, states, "*I offer technical support to the Director and the deputy directors. I also monitor government policies related to passport issues. Then, I also do interviews for passport application queries. Those who are affected, they come here. So we interview them*".

E11 also adds, “*My main responsibility is to see to the management of in-house developed applications and facilitate the development of user requirements for applications that are off-the-shelf applications the organisation wants to go by*”.

On compliance enforcement, E6, and E9 identified that role. E6 for instance, highlights that the main role included investigation of all digital crimes and supervising that data protection is enforced. E6 states, “*I investigate cases, and the evidence that we retrieve is people's private data. So, I need to make sure that apart from ensuring that data protection is enforced, most often, we deal with electronic evidence. So electronic evidence is very sensitive, and we need to protect it*”.

ISM Senior Management Roles:

On the senior management roles, some respondents indicated that senior management is involved in monitoring the attitudes of personnel to secure the data and reporting it for management to resolve them. For instance, E3 and E4 state the following:

- E3: *There are standard operating procedures that have to guide every registration, and Senior management must ensure that these standard operating procedures are followed and adhered to in their various departments. Once these are followed, then you minimise the risk. You minimise the information discrepancies, data redundancies, and all that*”.
- *E4: The senior management, as we know in every sphere, is to provide oversight and ensure that those that have to carry out tasks in relation to security carry out the tasks. There are organograms stating people's positions and what they should do, and they are given objectives to achieve throughout the year by means of appraisal and all that*.

Some respondents further believe that the Senior management role in ISM is to provide the required resources for its implementation. E1, E2, E6, E11 and E12 agreed on this. For example, E1 and E2 state:

- *E1: They make sure the tools and equipment needed for security stuff are available, funding and all that. They avail them.*
- *E2: They provide the minimum resources for administrative, organisational and technical controls*

Other respondents highlight that senior management ensures adherence to IS Security activities or programmes. For instance, E5 argues that "*The role [of senior management in IS] includes putting in the appropriate policies and measures to make sure that personnel adhere to those policies and go along with the policies to secure our information security.*

E13 also adds*, "Senior management supports Vodafone Ghana's security programme*".

On the senior management role in ensuring awareness of ISM, E7 states, "*Their [the senior management role in IS] role is to make sure that whether there is a breach, they are fully informed. Their role is actually to make sure that the organisation have what it needs to secure taxpayer information"*.

Some respondents believe that the senior management ensures collaboration with other organisations as a tool for ISM. On this, E9 and E10 agreed. E9 for instance notes, "*It's collaborative* [with other organisations]*, and we have direct reporting lines to executive management* [of our organisation and others] on data security. So it's collaborative and, of course [we do all these], *with executive management and direction and advice"*.

Finally, some respondents believe that as part of general IS security, it is the role of senior management to ensure the funding, development and approval of the organisation's ISP. On this, for instance, E6 sums it up and states, *"They [referring to senior management] bring in the policies. They must approve of the policies. So it's very, very key. If they don't approve of the policy, it'll not fly. So, they have a very big role to play. As much as they don't need to be technical people, they should have some knowledge, such as in budgeting issues, because they approve of the budget. So if they don't give you all the necessary budgets that you require, it might be difficult for you to operate".*

NIA Relationship

Relationship with NIA

The respondents highlighted that the relationship between their organisation and the NIA relates to data verification, authentication and integration. For instance, on authentication and integration, E1 states, "*NIA is a huge institution in Ghana, and I think we got to involve them in a recent project we undertook. The government has come forward with a new national ID card, the Ghana card. And that would be the form of identification in Ghana. So some of the things they're doing are ensuring that, for every Ghanaian that comes to the bank, we'll be able to authenticate that person via the NIA platform. So there have been lots* *of integration between us and NIA, and then another vendor called Margins to ensure that when these people come, we can authenticate their ID cards before they go through any transaction*".

E2 acknowledges the verification role and asserts that the NIA is "*to provide biometric verification services to all User Agencies, including Banks, through the use of information and communication technology infrastructure, data capture systems, card issuance systems and data exchange Web Services*".

E12 also asserts that their organisation's relationship is for individual or customer identification purposes. The respondent states, "*I think the basic relationship is on individual identification because we do have customers and clients, and to deal with such entities, you should be able to identify them. And we rely on a reputable third-party institution to vouch for the identity of these individuals. And they do that through the issuance of the national identification cards. So we rely on the card to identify an individual, trusting that the identification authority has done the various checks to confirm that the names these particular individuals are saying belong to them, indeed, who they are. So, the relationship is to identify the customers we deal with and any other entity or third party we deal with to identify them*".

Some respondents, including E3, E4, and E5, also acknowledge that their relationship with NIA is on data sharing and collaboration. On this, E4 for instance states, "*When we [referring to his organisation] onboard an employee, NIA will verify that the employee is duly Ghanaian when all other things considered have been verified, before the person will be allowed onto our system"*.

E7 adds that in addition to data sharing and collaboration, their organisation is mandated to adopt the NIA ID number (PIN) as the Tax Identification Number (TIN) of applicants for revenue mobilisation purposes. E7 states, "*We rely on the NIA for the national identification card numbers. The National Identification Authority is an ID issuing authority, and the GRA is a revenue mobilisation authority. And so, in terms of relationship, there is a direct relationship. However, the commonality between the GRA and NIA is that NIA, as a national identification authority by law, is that the GRA has moved towards using the national identification numbers as its tax identification number (TIN). And that inherently marries the two organisations as we have a common number. And this is happening in all the digital spheres of the government across the country"*.

Some respondents also believe that their organisation requests for information from the NIA about applicants for crime-related cases. For instance, E6 states, "*We've not had a situation where they have reported any case to us. So, the presumption is that they have not experienced any incident that may be considered criminal. So they've never reported, as far as I am aware. I mean, I'm the first head of the unit, so I don't remember receiving any criminal cases from them. But for us, all we do is request some information on some cards that we want information on. That's it*".

Formalised/Non formalised Relationship

On whether the relationship between external organisations is formalised, respondents were divided. While the majority of respondents believe that to be so, other respondents believe otherwise. In addition, some were unsure of the existence or otherwise of such formalisation as detailed under the various relationships below:

- ***Formal relationship***

E2, E3 E4, E5, E8, E9, E10, E11 and E12 indicate that their relation is formal. For instance E2 and E3 respectively state that "*Yes, both Law and regulatory requirements through ACT*" and "*Yes, it is bound by law. There is a legal framework that is establishing that relationship*".

- ***Not sure of Formal relationship***

Some of the respondents like E1 were unsure whether the relationship is formalised. E1 for instance states, *"I'm not sure if there's a law per se, but there's an agreement between us, that is, the bank and the NIA*".

- ***No formal relationship except general agreements***

E6, E7, and E13 believe their organisation does not have formal relationships except with other general laws. For instance, E6 sums this up and states, "*We don't have any direct relationship with them. The only thing that may bring us a little closer is a request for information on, maybe, a card that we want to validate*".

E7 adds, "*I believe that it [the relationship] must conform with ACT 843 of 2012. This Act protects the privacy of individual and personal data by regulating the processing of personal information. The Ghana Data Protection Commission provides the process to obtain, hold, and disclose personal information for all Ghanaians. So, we use their leadership to guide that there's harmony across the board concerning data protection and the policies we generate*".

Functional Reliance

On the functions that the external stakeholders rely on the NIA for, respondents assert that they rely on the NIA to verify their customers' information. For instance, E2 states that their organisation relies on the NIA *"Primarily for verification. When operational, it [the NIA system] will become the de facto identification system for verifying the authenticity of holders of bank accounts in certain financial transactions*".

E11 and other respondents also noted that their organisation rely on the NIA for the purposes of identifying and verifying customers. E11 for instance, states, "*As far as I know, it is for identifying and verifying our members*".

Other respondents also acknowledge that their organisations rely on the NIA for authenticating their customer details to prevent impersonation. For instance, E1 states, "Everything that you do, like if you're making the deposit, you need to be authenticated. Again, If you're making withdrawals, you have to be authenticated to know there is no identity theft. So those are the things that we need to do. So, in that aspect of authenticating, you check in to ensure that this is the person. I mean, this card that the person is using is that person and is not that the person has been impersonating or something".

Some respondents acknowledge that their organisation relies on the NIA for the validation of data. On this, E3 states, "*The NIA will rely on us for new birth registration, and then we'll rely on them to validate the NIA IDs of parents who come to register their children*".

Other respondents indicated that their organisations rely on the NIA to carry out their mandate. For instance, E5 explains, "*My organisation is sharing data with the National Identification Authority. It helps us identify the foreigners and foreigners who are in the country and give birth*".

Other functional reliance, as noted by respondents, relates to enhancing data integrity and facilitating the organisation's operational functions. On this, for instance, E10 states that "*first, it [the organisation functional reliance on NIA] enhances our data integrity. And the second, it also speeds up our work. It helps facilitate our work so we don't need to go through other means of conducting checks, which sometimes takes a week or two weeks. With just a click, you'll be able to get other information from the NIA. So the speed of our work and our operations are enhanced. For now, these are the two basic things*".

Influence on NIA Operations

On the external organisations' influence on the NIA operations, most of the respondents answered in the affirmative. Some indicated that they have formal representatives on the NIA Board to achieve such influence. Some of respondents who supported this position included E2, E3, E5, E7, E8, E9, and E11. E3 for instance, asserted that "*Yes, it is bound by law. There is a legal framework that is establishing that relationship*".

Interestingly, some of the respondents answered that they have formal representation through Memoranda of Understanding (MOUs) and are complying with some directives. Such respondents included E4, E10 and E13. For instance, E13 states "*No, it is not [formal]. It is an MoU we signed with them. There's an MoU signed that enshrines our relationship with them"*.

Other respondents highlighted that they do not influence the operations of the NIA. Such respondents included E1 and E6. E6 for example states "*We don't have any direct relationship with them. The only thing that may bring us a little closer is a request for information on, maybe, a card that we want to validate*".

6.5.1.3 Information Security Policy

The ISP covered eight themes: ISP importance, ISP Status, ISP Awareness, ISP content, ISP Development Process, ISP enforcement, and ISP evolution as shown below:

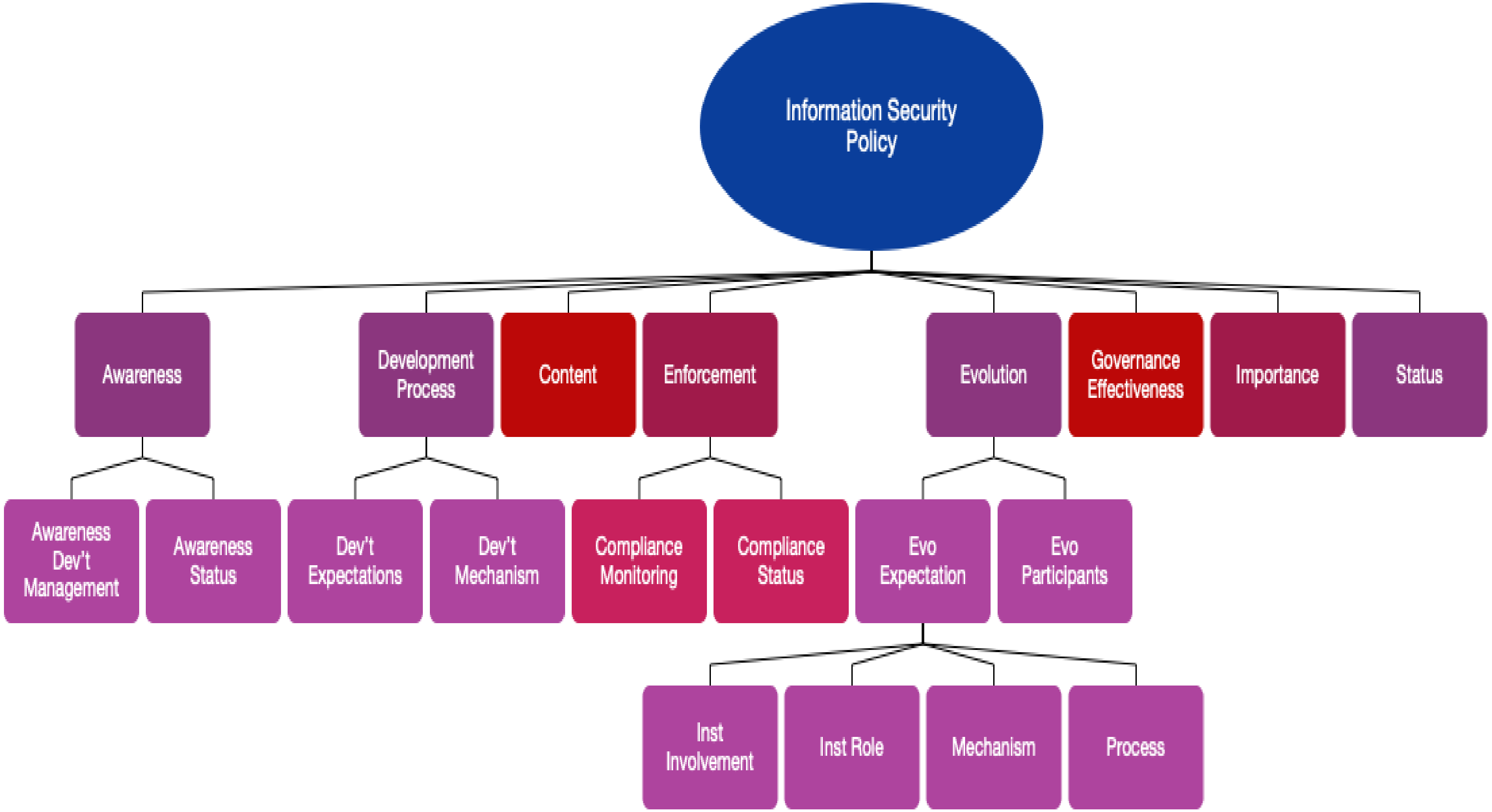


Figure 22: ISP Category, eight themes, subthemes and subtopics

The detailed analysis of each of the themes is as below:

A. ISP Importance

As noted in the previous chapter, the ISP Importance theme covers respondents' views on the importance of ISPs relative to individual, organisational, national, and general benefits.

Regarding individual benefits, the respondents' view highlights that the ISP serves as a guide to ensure the security of individuals' data and its management. On this, for instance, E8 asserts, "*It's important. It is hugely important because; a policy is what guides everybody so that everybody knows how they should carry themselves as far as information in the organisation is concerned*".

E10 also noted that the ISP helps to prevent unauthorised access to data by individuals and stated "*It is very important because we manage people's personal data and once you don't manage it well and they get out there, there are other unauthorised institutions that may lay hands on this information which doesn't speak well of us. And then if some of the individuals get to know that their personal information have been shared with the public and other unauthorised persons, they can take these issues to court so this is very important*".

Other respondents like E3 note that, by the nature of EIS organisations and changes in technology, ISPs help protect an individual's identity. He states, "*Identity issues are evolving. And they are people's personal information that if anyone gets a chance to have, it can be used to do so much to the individual. So critically, it is important for the national identification office to have the ISP in order to basically guide every organisation that is keeping some form of data since they are mandated by law to be the national data repository*".

Regarding organisational benefits, the respondents indicate that the ISPs are important as they serve as the standard for effective compliance. For instance, E1 and E2 respectively state that:

- *E1: It [referring to the ISP existence] is very important. Information Security policy is the standards or procedure that when incident happens, those are the things that we follow through. So these are things that should come handy to ensure that all security issues are tackled if the needed reactions.*

- *E2: It's [referring to the ISP existence] the foundational management intention to its staff and other stakeholders on the level of importance it attaches to information Security.*

Other respondents believe that the ISPs contribute to the realisation and achievement of organisational objectives. On this for instance, E13 states, "*It [referring to ISPs] ensures the realisation and achievement of captured functional objectives of the programm*e".

In addition, respondents indicate that ISPs facilitate the relationship between an organisation and its relationship with external stakeholders. For instance, E2 states, "*It is absolutely important as it will help in the management of their relationship with internal and external activities of the organisation*".

Some respondents highlight that the existence of ISPs is important because it serves as a guide for ID management organisations' systems. A respondent, E3 for instance state, "*It'll guide the entire process of the ID management systems. It'll set controls, it'll set standards that will guide the identification processes. It'll also spell out protocols that will guide user agencies*".

Regarding national benefit, some respondents assert that there should be ISPs to protect national data, revenue improvement and the security of the state. E5 for instance, state, "*policy [referring to ISP] will guide the NIA and for that matter, the nation. This is because they're taking data on all the population of the country. And for that matter, if they don't have an IT policy, anything can happen to the data and the information of the country or the security of the country can be jeopardised. So it is necessary that they [referring to NIA] have it*".

On revenue improvement, E7 and E8 state that:

- *E7: The efficiency of their security policies is extremely important to us because we rely on them to register new taxpayers and get taxpayer-updated information from them. If anything happens to them, that means we'll not be able to register new taxpayers, which is not efficient.*
- *E8: It [referring to the NIA ISP] does impact positively because it has led to the identification of individuals who were not heather in the database of GRA. They have helped GRA increase the number of people who should be or are potentially liable to pay tax. And so, it has had a positive impact on the GRA.*

Regarding other general benefits of ISPs, some respondents indicate that the ISPs could guarantee an extent of privacy and trust in their organisation's use of data. For instance, E9 states, "*I believe once we conform with the data protection act, we are guaranteeing that individuals data is private, kept confidential, both in transition and operation. For our operations, we need guarantees about the privacy of the data being maintained*".

B. ISP Status

On the ISP status, the analysis from the external stakeholders highlights two general observations. The two observations were those who believed in the existence or expected that the NIA had an ISP, while the second were those who were not sure of the existence of an NIA ISP. However, the majority of the respondents believe that there is an existing NIA ISP or expect the NIA to have an ISP. Interestingly, all except E2, E5, and E13 answered in the affirmative on either the existence of an ISP in NIA or their expectation of NIA having an ISP. For instance, E6 asserts that "*Why not [in response to whether the respondent believes the NIA has an ISP]? I think I have indicated that they are critical information infrastructure and any breach there have serious consequences for us as a nation. So they should have security policies. They should make sure that they do risk assessment, risk management and all that risk analysis*".

In the case of respondents not sure of the existence of ISP in the NIA, E5 for instance, asserts that "*Till date, I don't think we have been engaged in any of such policy before. So, to me, I don't know whether they even have a policy because we've not been engaged and as stakeholders, especially formalised stakeholders, we would have been expecting that if they have such, we should be involved in it: in the drafting of the policies or in reviewing those policies*".

E13 adds, "*I cannot know as we have not been engaged in its development or amendments to it*".

C. ISP Awareness

The ISP awareness focused on two identified sub-themes based on the participants' responses. The sub-themes included ISP Awareness expectation and Awareness status. From the participants' responses, we can say that the external stakeholders identified training, education, sensitisation, capacity building and informing employees and stakeholders as ways of facilitating general ISP awareness and compliance as far as the ISP awareness expectations are concerned. In addition, the respondents largely expect the NIA to ensure the awareness and compliance of their ISP by using other strategies such as the adherence to protocols on data protection by individuals, data protection rights and privacy, recognising the importance of staff roles and testing the understanding of stakeholders. The details of the sub-themes are as below:

- ISP Awareness Expectation

On training, E1, E10, and E12 among others highlighted the need for it as a tool for ISP awareness. For instance, E1 states "*There should be trainings organised for the team on security awareness. If possible you can even take exams because these are important. One person alone can just cause a whole lot of issues. So it's very important that trainings are done, awareness teasers are organised. That's what we call Teasershere*".

E10 also adds, "*Training is one of them as it cuts across everything so that they will know what to say in public and what not to say and how to also get them vested with their document security. That's the document security training helps them on how to keep documents, where to put each one and where not to put each one. So the document security also come in place. And, uh, Basically that is it"*.

E12 adds, "*They should do regular awareness training with their staff through different media. It could be through email, face to face training, induction, text messaging, online quizzes and stuff like that. I mean, they should try all various avenues to ensure that their staff are well trained when it comes to information security matters*".

Other respondents such as E2, E4, E5, and E9 highlighted education and sensitisation as tools for ISP awareness. On this for example, E2 states, "*I think that there's more sensitisation to be done. Even with the public, for now, they know they have to go and get NIA card. But they don't have information on how the card is supposed to be used….So there's the need for continuous public education*".

E4 adds, "*There ought to be some sort of sensitisation across the organisation just like any other security policy when it is released. So you plan for the people and then you meet them face to face or by whatever means, explain the policy to them, get them to understand the policy as it governs their operations and security policies govern every aspect of the organisation. So, nobody should be left out. It shouldn't just be an IT thing*".

E5 also adds, "*Based on my experience, there should be continuous education to the internal staff, and they should make sure that all the users of the system should also comply. What I mean when i say they should also comply for instance is that, if I'm coming on to log into a particular machine, I need to put in my credentials. So they should make sure that all the machines are supposed to have accessing credentials before you can access the machine*".

Another ISP awareness expectation tool identified by respondents is capacity building among the stakeholders. E3 explains that the NIA can use capacity building to ensure staff awareness and compliance and states, "*Through capacity building. For the staff, it is capacity building. For the general public, it is sensitisation. They need to engage the community leaders. You know, over here, community leaders' leadership plays a key role when it comes to educating members of the community. So they need to engage with the community leaders, the chief, the opinion leaders. They need to bring them to a platform to understand. Once they understand, the message will go down*".

Respondent E7 also asserts that adherence to protocols on data protection by individuals, data protection rights and privacy, recognising the importance of staff roles and testing the understanding of other stakeholders can help in awareness and enforcement of the NIA ISP. The respondent states, "*I think that there are two key things when it comes to data protection. I think that there are two key stakeholders: the individual and what rights they have to their data and the privacy of their data; and then we have organisations and how they use the data. I think that the law is very clear about the protections that it provides. And so with that, it is very, very important for organisations too, to adhere to protocols that enshrines the safety of citizens. Given that every single Ghanaian's data is with them and given that the staff do have access to the data for every single Ghanaian, it becomes extremely incumbent for them to be able to enforce their Policies and then to test the various tenants and the stakeholders of what makes that policy and I think that it is extremely important to be able to make that happen*".

Interestingly, a few respondents including E6 and E11 have different opinions. For instance, E6 indicates that because his organisation does not interact directly with the NIA, the respondent says he is unable to answer questions related to staff awareness and compliance by stating, "*I don't know about them. So I can't answer that question*".

Respondent E11 also states, "*It [referring to Awareness and compliance to NIA ISP by staff] would be difficult*".

- Awareness status

The respondents believe that there is general awareness of the organisation’s ISP. Some of these respondents included E1, E8, E9, E10, and E12. For instance, E1 states “*Of course, when we do meet. I remember when we were doing the setup, we interacted with them a lot and then some of the things they insisted meant that they knew what they were doing about security*”.

E8 adds that “*Oh yeah I think so [referring to the awareness]. Like I said, they won't even allow you to assist them when even there's crowd. The GRA officers are complaining because they themselves are not allowed by the NIA staff to assist. Even though they're here and the bosses are not here, but because they have been told that this is what you do because of the security of the information you're dealing with they stick to it and they will make sure that no matter how stressed they are as a result of the traffic for application of the Ghana card, they just don't. They will never, never allow anyone to do what they not supposed to be doing. So I think that to that extent, yes, the NIA officials that are doing their work are complying with whatever guidelines, if there's any that they've given them*”.

Other respondents also believe that though there is awareness of the ISP, it needs some improvement because it is average. Such respondents for example were E2, E3 and E7. For instance, E2 states, “*So far, I believe it is an averagely okay as I am yet to know any serious breach though registration chaos is a concern at the moment*”.

E3 adds “*There is some kind of monitoring that is going on. For instance, NIA when they're having challenges with validating the birth certificates that have been presented to them, there is a mechanism for them to get in touch with us to do that for them. But as we speak now, it is done not electronically by manually. For it to be effective and for us to have an effective monitoring mechanism,this is supposed to be done by a click of a button. But we are not there yet, but there is some kind of mechanism for monitoring*”.

Other respondents do not even know the status of awareness due to their non-interaction with the NIA Staff. Examples included E4, E6 and E11. For instance, E6 states “*We* (referring to his organisation) *dont interact with them”* [referring to the NIA Staff].

E4 adds “*We* [referring to his organisation] *have a link with them for the work of accountants. We are their accountants…And we have accountants over there, but as to whether we understand their operations, we don't. We have to get to understand*”.

E11 adds "*Personally, I have not had enough experience with their staff [NIA staff] for me to be able to answer as to whether their compliance to their information policy is effective or not*".

D. ISP Content

Regarding the ISP content, respondents highlight that an EIS ISP like the NIA ISP must focus on critical issues such as network security, personnel security, software security, policy management, data sharing, general security management, access rules and employee conduct. Other aspects the respondents highlighted include physical security, application security, data life cycle management, employee education, and satisfactory legal & statutory requirements as well as business continuity.

On network security, some respondents indicate the need to ensure the provision of firewalls to protect the data and the system. For instance, E1 states, "*Since we are actually connecting to them via a VPN or via the network, I think, security around the network protection is very key. So there will be the need to deploy a firewall for filtering purposes, and then also, there would be the need for them to put in place measures to avoid eavesdropping or maybe manage the middle attack as in data transmission between us and them*".

On personnel security, the respondents believe that procedures on attack prevention and intrusion detection strategies should be essential in the ISP content. This, they believe, would enhance the organisation's security. For instance, respondent E4 notes that the personnel must be scrutinised to ensure that the quality of personnel recruited are up to the task and have the integrity and states, "*The employees who work at the place should be scrutinised. Their background checking should be done very well so that in this age of politics where people can cause mayhem, they will be held responsible and they will be doing things per the law and not outside of it*".

On the need for intrusion detection and protection, E1 highlighted that "*For information security policy, first of all, there should be procedures on how to prevent any form of attack. And then also once you are attacked, how to kind of remediate them. That's the intrusion detection and then intrusion protection. These are very key components*".

On software security, the respondents note that the ISP must be clear on the standard software for efficient data synchronisation and data sharing. For instance, E3 explains "*It [referring to ISP Content] should be clear on a standard software that that should guide every* *agency's operations. Agencies that are collecting some form of data on individuals, there should be a standardised software because if you talk of integration and there are different software, it makes integrations sometimes a challenge. Although there are APIs that can connect different form of databases, but if they can come out with a standard, it may not be one software, but the same software will be the same standard that will guide operations. And it must also spell out the protocols. The protocols must be clearly spelt out. What you need to do at each stage of the operations when it comes to especially taking biometrics and taking individual information. The ISP should state clearly it should have a clear guide because as we speak now, every agency is taking biometric data using different formats to take biometrics, and that is not helpful*".

On policy management, the respondents highlighted the need for the ISP to focus on a clear mission and vision to achieve organisational objectives. On this, for instance, E2 identified that the ISP should focus and prioritise "*Key policy statement, roles and responsibility, objectives of the information security policy and how it intends to achieve those objectives*".

E3 adds that standardising key concept definitions as part of the ISP content, its purpose and responsibilities among others would help in the general management of the ISP and explains "*There should be standardised definitions. For instance, if you say biometric, there should be a standard definition that should cut across. If you talk about internet security, it should have a standardised definition. All these things should be clearly spelt out so that there is standard that will guide all agencies. It should be very clear*"

E8 also explains that the ISP "*should state the intent, what it seeks to do, the purpose, and then it should inform staff as to how, the information in the organisation should be handled. I think the policy, should indicate the dos and don'ts on the part of staff in handling information, how they should relate with even external stakeholders and internal stakeholders as well in handling information. And I think these are the key things that should go in there to ensure the sanctity of whatever information that they're holding*".

E12 also adds, "*It should states the rules and responsibility of the individual who is to run the information security programme. It should have Acceptable use of information assets, what to do, what not to do with asset or information assets. How should the information assets be protected, backup, disaster recovery, things like that on a higher level to protect Information assets".*

Regarding data sharing as part of ISP content, the respondents note that the policy should specify data sharing specifications, requirements and limitations relative to the internal and external partners. Respondents such as E4, E5, E8, E9 and E10 share this view. E8 for instance asserts, "*When it spells out the conditions of data sharing, the extent to which each of us can access the information, how we should still have access without injuring the sanctity of the information and the protection. It could also contain if any, Concerns about cost. It should be properly documented, and so that we all know how we can partner each other to effectively work together*".

Other respondents believe that the ISP content should make provision for other general security management, including having a backup. E5, for instance, states, "*We look at access to their data centres, or their server rooms, and do we have backups somewhere? Where are the backups? Are the backups at places which are not even known to people and other things?*"

Some respondents also suggest that the policy should cover the access rules and employees' conduct. For instance, E5, states, "*We will be talking about the access to the information because we are sharing data with them. It will be very key. And then, also looking at their a access control levels, and also looking at the secure nature that the data can be transferred because it is electronic data. Whether the data is encrypted or not, you may not know. And then the user access level should also be looked at*".

E13 adds that the ISP content should focus on "User Access, Acceptable Use, Network, etc especially on user access and network as it directly affects our[his organisation's operations]".

Regarding physical security, some respondents assert the need to ensure physical security strategies as part of the ISP content components. For instance, E6 states "*You want to look at the network, you want to look at applications, you want to look at physical security, everything*".

Additionally, some respondents believe that the ISP content should cover all aspects of application security. E6, for instance, states, "*So far as it's a critical information infrastructure, we expect that they should have policies that would cover physical security, network security, all aspects of the application security*"

Another highlight from the study shows that the content of the policy must focus on data exchange, transition and at rest (redundancy). On this, E7 explains that the ISP should focus on "*Every aspect of pretty standardised security policies: in terms of how data is exchanged, transited, at rest. I think all of these things are very much important. Who have access to data ,who can see the different aspects of the data, sensitisation, organisational policy with respect to equipment, machines coming in etc. So for NIA, instituting policy should be a very thorough end-to-end approach. And I think the same thing applies to us at GRA*".

Regarding employee education, the respondents highlight a need for a provision in the ISP content to educate staff about the organisation's ISP. A Respondent E8 states, "*The understanding and appreciation of the staff is very essential because we work with them. And I guess once everybody knows their policy, the policy on the information they are gathering, we will have a better relationship with the NIA in our collective quest to ensure that acquisition of the Ghana card is facilitated and for that matter, the identification of taxpayers is also facilitated*".

On legal and statutory requirements, some respondents believe that EIS Policy content must be strictly done to conform to established local and/ or international standards. On this, E9 states, "*You* [referring to the assessor of the ISP] *expect that it conforms with the Data Protection Act, and it gives guarantees and assurance to the public, on how secure their data is and how private it is, and offers them some form of accessibility to their personal data and allow them to be able to update as and when it is wrong and be able to give guarantees on third party sharing of that data and controls around it*".

E1 also adds that *"So I think, one of the things for us that we look for before we start working for anybody is that we look out to shape whether they are compliant with certain standards, like ISO standards, PCIDSS and then the kind of policies that they have implemented, the standards that they follow does the NIST standards and some other practical standards. So, obviously they need to look out for these before they onboard any other vendor or any other customer. They need to ensure that these people are complying with these standards to give them the assurance that there's some level of security so that these other people that onboarding will not be like security points where they're gonna have issues with. that's entry point of security lapses".*

Respondents also believe that, the ISP content should have the organisation's business continuity process as part of it. This is to ensure the integrity of the organisations involved.

On this, one respondent, E11 states, "*I feel that business continuity is something that is very important. And because we depend on them, .how they manage business continuity is very essential to us. And then also how they're managing, confidentiality, integrity and availability of the information is something that is essential*".

On the key provisions for the NIA ISP content, the respondents focused on varied opinions as detailed below:

- E1 focused on data management and incident prevention, key and states "*key will be the data management and then incident prevention*".
- E2 focused on "*key policy statement, roles and responsibility, objectives of the information security policy and how it intends to achieve those objectives*".
- E3 also highlights that key provisions should focus on "*the security protocols, connectivity protocols and data sharing protocols*".
- E4 focused on protection of personal data and states "*Issues of Personal information should be looked at. Whatever policy should actually take a good look at the personal information of people so that these information will not be leaked or maybe even the perimeter of NIA should be governed in such a way that there will not be any unwarranted intrusions into the system to steal the data"*.
- E5 focused on access control and stated "*We will be talking about the access to the information because we are sharing data with them. It will be very key. And then, also looking at their a access control levels, and also looking at the secure nature that the data can be transferred because it is electronic data. Whether the data is encrypted or not, you may not know. And then the user access level should also be looked at, to mention just a few*".
- E10 also focused on data protection and cyber security and states, "*Data Protection and cyber Security. I think for now the two of them will be okay: the data protection and cybersecurity is okay. Because it involves the transfer of information from one institution to other. Therefore the cyber security will also be there, because alongside, we make sure that we don't expose our system to other unauthorised actors. But with the data protection, it's also very important. I think the two of them they're all very important"*.
- E12, however, focused on management roles and responsibilities in ISM, acceptable use of information assets and asset management and states "*They should have things*

about one, What is management's position on information security. What are the rules and responsibility of management? It should states the rules and responsibility of the individual who is to run the information security programme. It should have Acceptable use of information assets, what to do, what not to do with asset or information assets. How should the information assets be protected, backup, disaster recovery, things like that on a higher level to protect Information assets".

E. ISP Governance

Regarding ISP governance effectiveness, the respondents were largely divided. Some respondents generally believe that the NIA has an effective ISP governance process. However, some respondents were unaware of the effectiveness of the ISP governance process.

Those who believe the NIA ISP governance is effective included E1, E2, E3, E5, E12 and E13. Some examples of their statements are as below:

- *E1: I believe they [the NIA governance processes] are effective since they're an umbrella team that does put together all these banks, and other corporate organisations. So I expect them to be effective.*
- *E2: [the NIA ISP governance process is] Significantly important*
- *E3: The effectiveness [of the NIA governance process] will be through a lot of sensitisation programs. The sensitisation program will make it [referring to the NIA governance process] effective.*

Those that were unaware of the effectiveness of the ISP governance process included E4, E6, E7, E9 and E11. Examples of the comments made are the following:

- *E4: I have no idea of their structure or how it is governed. The question you have asked me is very important. We have to get to understand how they operate so that when we are relying on them, we know that they are actually taking care of us. Just a verbal assurance is not enough. We have to look at the processes and get to understand how they work".*
- *E6: I can't answer that because I don't even know the policy.*
- *E7: I don't know. I don't work in the organisation so I wouldn't know"..*
- *E9: I would say I'm not privy to the governance process so I couldn't really give an opinion on that.*

- *E11: I'm not too sure of the governance process there. So, I am not able to answer that question.*

F. ISP Development Process

Based on the responses, the research identified sub-themes on the ISP Development process. These sub-themes included ISP development expectations and ISP development mechanisms.

- ISP Development Expectations

On the ISP development expectations, we asked respondents whether their organisations' concerns would influence the development of the NIA ISP. On this, majority of the respondents believe that their organisations' concerns would be considered or would influence the NIA ISP development process. They highlight that, by the nature of their reliance on the NIA for service provisions to citizens and the need for collaboration with the NIA, their organisational views would be a key factor. Some of the respondents included E1, E3, E4, E5, E6, E8, E9, E10, E12 and E13. For instance, E3 acknowledges this and states, "*I believe the policy is not just going to be useful for only NIA and so there should be a lot of stakeholder engagement so that the policy will cut across both the agencies and the users. Every stakeholder that has something to do with vital information on individual should be consulted and their input be fed into the ISP"*.

E4 adds, "*Our concerns should be somehow addressed by the policy when it is crafted. The whole country depends on us for the payment of civil servants. It'll be in our interest to ensure that whatever NIA comes out with will also address the concern of civil servants in the area of the security of their information. That is where our stake is*".

E8: "*To the extent that now we have adopted the Ghana card personal identification number (PIN) as TIN, definitely we will be happy to have our concerns considered in developing any policy*".

However, E7 refused to comment on the development of the ISP.

- ISP Development Mechanisms

Regarding ISP Development mechanisms, the majority of the respondents believed that there is no mechanism used for their organisations' concerns to be considered /influence the development of the NIA ISP. However, few of the respondents believe that there is a mechanism. Those who believe in the existence included E8, E11 and E13. On this, E8 for example states, "*The GRA had a memorandum of Understanding, but we will revisit it*".

E13 adds, "*The only mechanism available is by Consensus meeting. We meet when we have issues or they have issues as detailed in our MoU*".

Those that do not believe in the existence of such mechanism included E1, E2, E3, E4, E5, E6, E10 and E12. Example of their comments are as follows:

- *E1: No, but of course, they can put out questionnaires with vendors or their customers. They can bring out questionnaires on the kind of security we expect them to put in place for us to be comfortable.*
- *E2: No. Currently, we only relate with them on the issue of verification of our customers using the data in their possession.*
- *E12: As it stands now, I don't think there's any mechanism. The only way is to level our grievances to our regulator who would intend pass it on to them because of their relationship from a state's perspective.*
- *Other responds were however unsure about the mechanism and state as follows:*
- *E7: I am not sure though we work closely with them*
- *E9: I cannot speak to that but I believe in having our representation on the board, I believe our opinions are able to come out as a formally.*

G. ISP Enforcement

The ISP enforcement theme focused on the external stakeholders' view on NIA's ISP compliance monitoring and compliance status sub-themes. Generally, the participants' responses indicate that the NIA ensures staff compliance through monitoring and awareness creation. However, some respondents acknowledged that the NIA has to improve its ISP compliance enforcement.

Regarding compliance awareness, the respondents were divided. Whereas some respondents believe that there is compliance awareness through training and sensitisation, others remained unsure in their responses. This means that though the respondents believe in ensuring the need to protect the confidentiality, integrity and availability of data to earn the trust of external organisations, there is a need to improve the enforcement of the NIA ISP both internally and externally. This is to ensure that all stakeholders are aware of the policy and that they are monitoring their employees' activities. To provide clarity, we will attempt to discuss each sub-theme in detail.

- Compliance Monitoring

Respondents indicate that there is some compliance monitoring in the NIA to ensure the enforcement of their ISP. E3 for instance, states, "*There is some kind of monitoring that is going on. For instance, NIA when they're having challenges with validating the birth certificates that have been presented to them, there is a mechanism for them to get in touch with us to do that for them. But as we speak now, it is done not electronically by manually. For it to be effective and for us to have an effective monitoring mechanism, this is supposed to be done by a click of a button. But we are not there yet, but there is some kind of mechanism for monitoring*".

Other respondents also assert the need to improve compliance monitoring through the enforcement of certain standards and technology. Some of such respondents included E3, E5, E7, E9 and E10. On this, E3 for instance, explains that "*The best way to ensure that compliance are effective will be through the use of technology because once you use technology, you just build in the constraints, and the constraints alone will make sure compliance are effective*".

E7 also adds, "*Yes [in response to the question on compliance monitoring]. Compliance is effective. It is not only important to monitor but to enforce it as well*".

Additionally, some respondents were however, unsure about compliance monitoring to the NIA ISP. These included E2, E4, E6 and E11. For instance, E6 states, "*I don't even know"* [referring to not sure if they have means of ensuring ISP compliance]

E11 also adds, "*Our information security policy is similar to what we have in ISO2700, which is a standard for information security. We believe that the NIA information security will also be in reference to similar standard and as such, our staff are measured and then guided by what we have in our information security policy which we believe to a larger extent will be similar to the NIA one*".

Some respondents also believe that as part of compliance monitoring, organisations such as the NIA should ensure active policy violation strategies and effective punitive actions. E12 states, for instance, "*So since most of the information security policy content is driven from* *the law, the NIA law, my or our suggestion would be that, to be able to ensure compliance NIA should implement the law to fullest so that those who fail to comply with the content can be given the penalties that the law prescribes*".

- Compliance Awareness

Respondents were largely divided on the compliance awareness of the NIA staff. While others hold the view that staff compliance awareness is present, other respondents were not sure about their compliance awareness.

For those who hold the view that compliance awareness is present among the staff of the NIA, they included E1, E4, E5, E7, E8, and E10. Examples of their statements included the following:

- *E1: I remember when we were doing the setup, we interacted with them a lot and then some of the things they insisted meant that they knew what they were doing about security.*
- *E1: I believe per their standards, they will follow through what the policy says. That's the standards like the ISO standards which talks about training of staff, user awareness and it is a very, very key component. The NIST also talks about that. So I believe if all these standards are adhered to, they will be able to follow through and then ensure their staff are pressed with security trends.*
- *E5: With the NIA policy, the relevant provisions are applicable to us and are enforced.*
- *Those that were unsure included E2, E6, E9, E11, and E12 and some of their comments were:*
- *E2: Not sure [in response to the question on compliance awareness]*
- *E6: We don't interact with them [referring to the NIA staff]*
- *E9: On a personal note, my interaction [with the NIA Staff] hasn't given me a reason to doubt that, there is an issue related to that [referring to awareness].*
- *E11: Personally I have not had enough experience with their staff for me to be able to answer whether their compliance with their information policy is effective or not.*

Some respondents, including E3 and E13, decided that they had no comment on that.

H. ISP Evolution

The ISP Evolution process discusses the NIA ISP expectations process, external stakeholders' roles, participants' evolution process, their organisational influence in the evolution process and mechanisms available.

The participants' responses indicated that they understood the ISP evolution process and expected that their views would be considered and would influence the evolution of the NIA ISP. They also acknowledged the institutional role that their organisations play in the NIA ISP evolution process which included policy inputs, providing feedback, implementation and coordination support towards ISP enforcement, among others. In terms of their expected process for the evolution, the respondents indicated the need to recognise legal and regulatory guidelines, liaise with the regulatory stakeholder organisations, recognise the environmental, social and technological factors as well as carry out consultations and stakeholder engagements.

In addition, some respondents suggested an annual risk assessment of the policy, and based on identified gaps, a review could be conducted by experts and the affected departments, or units or stakeholders.

Regarding the evolution mechanism, the respondents were divided with some believing that there is a mechanism while others believed otherwise.

Under the evolution participants, the study identified four opinions. These opinions included:

- Believing in delegating a team of internal stakeholders to collaborate with the external stakeholders to review the ISP;
- The internal organisation liaising with the external stakeholders' regulatory organisation;
- Bringing all identified external stakeholders together to discuss and review the ISP;
- Bringing everybody to participate in the review process.

The details of the ISP evolution sub-themes are presented below:

Institution Organisational Influence: Generally, respondents indicate that they expect their organisational concerns to be considered or influence the evolution process of the NIA ISP. These respondents included E1, E2, E3, E4, E5, E6, E8, E9 E10, E11, E12 and E13. On this, for instance, E8 states, "*I expect our concerns to be factored when they're developing any* *information security policy. In the same manner, there should be stakeholder engagement with us when there is the need to do any amendment. It'll not be good for NIA, to just unilaterally amend something that together with them, they developed. So the process should still involve stakeholder engagement to enrich the amendment*".

E2 also adds, "*Yes,* [in response to the question on whether they expect their concerns to be considered or influence the NIA ISP evolution] *but likely through Ghana Association of Bankers (GAB)*".

E9 also adds, "*Yeah* [in response to the question on whether they expect their concerns to be considered or influence the NIA ISP evolution], *I would expect that our inputs and views would be reviewed, for appropriateness*".

Institutional Role: Respondents such as E2, E9, and E11 expect that their institution either make some inputs in the review process or provide feedbacks. For instance, E2, states "*Make our inputs or feedbacks known to them likely to be through Ghana Association of Bankers (GAB)*". E9 adds, "*I believe as a consumer of the data, we would make our inputs as and when necessary and as a stakeholder*".

On the feedbacks for instance, E12 states, "*As stakeholders, we should be able to provide a feedback that would go into the evolution. So if there's any shortfall that we identify, it should be our duty to report back to them so they can incorporate that into the next iteration of their policy*".

Additionally, other respondents believe that part of their expected role would be coordinating with the NIA to enforce the NIA ISP. For instance, E6 states, "*We should be able to also review their policies and advise them accordingly*".

Further to the above, some respondents believe that their organisation has to be a participant in the whole evolution process. E1 for instance states "*Of course. They have to work with stakeholders, like us*".

E3 also explains, "*We are the organisation that produce the breeder document and we get in touch with every individual that comes in and any individual leaves. We take account of it. So we are very critical when it comes to things critical to them. For NIA to be able to update their systems, we play a critical role, because we can tell NIA that for this quarter, Y number of* *people have left, X number of people have been added. So my organisation would have a lot of influence when it comes to the update of NIA records on Data*".

E10 also adds "*We should be part of the stakeholders when they are having meetings. Passport office should be invited*".

Interestingly, some respondents however do not know anything about the evolution process of the NIA ISP. On this for instance, E13 states, "*No idea as I have not read their ISP*".

Evolution Process: On what respondents expect to be the process for the NIA ISP evolution, some of the respondents indicate that they expect that the process would involve engaging their organisation through their regulatory bodies. For instance, E2 states that, "*I believe that the NIA would likely want to relate with us through Ghana Association of Bankers (GAB) on such issues*".

Some respondents also acknowledged that the process must consider the environmental, social and technological factors that the institution or organisation operates in as part of the evolution process. They believe that this could be achieved through consultations and stakeholder engagements. E3 states, "*I believe that implementing agencies like NIA should look at their environment and look at the culture within their environment to be able to update their ISPs. It shouldn't just be that because technology has evolved, things have to change. I don't believe in that, but looking at the current trends within your country. This is because society has even changed. Even the naming systems in the countries have changed and all that. For instance, you find one name with different spellings. And you even find organisations using very old software that are still usable for them. They need to really do a lot of consultation and stakeholder engagement*".

E4 adds, "*The NIA should have, let me put it in the local parlance, "an open ear" to the stakeholders in their data and ensure that they listen to them and, take on board what they say so that when they are updating the policy, they will include some of those things. I will say that at the beginning, we cannot over everything but as we go on, we'll be fine-tuning the process and getting people's view into it and getting things to work better than before*".

E9 also adds, "*Policies are living tools, and as the environment changes and things change around us, I believe they get reformed, and the reformation has to go through the various* *stakeholders that play a role in getting the national identification grounded and functional. You would naturally expect that the stakeholders will participate in the policy formation and be consulted on them*".

Some respondents also believe that the Board of Governors must be informed and all other stakeholders involved in the evolution process. E5 for instance states that "*There is a need for their Board to be informed that, all stakeholders should come on board for them to amend or for them to come out with such policies so that we will all contribute to it because we are all stakeholders in that matter*".

Other respondents assert that there should be yearly risk management assessment to identify policy gaps and based on that, then they involve the relevant stakeholders. On this, E6 states, "*There must be a review of the policies regularly which should go alongside with risk management so that as they look at their risk assessment. From their risk assessment, they'll be able to incorporate how to manage them in the new policies that they will have to be running every year. So it is supposed to be a comprehensive thing and they should get all their stakeholders involved, getting all their stakeholders involved is also important because any of them could be a conduit and again, because we are all going to assess the data. We should all be involved so that we get to know the policies that they are running with. This helps them to as well know how we are accessing the data. We also get to know what privileges we have. And if we have any concerns, I believe that we raise it*".

Some respondents also believe that the process should include the involvement of the general public using technological advancements like web portals or their websites. On this, E12 states, "*There should be a portal either on their website or wherever where people can look at what they have now and perhaps contribute to any changes that should go into t.he work. So if there's a portal that they've displayed their information security policy, interested parties will be able to tell if it's adequate or it will require some input. And then the portal should also provide the avenue to give that input*"

Evolution Mechanisms: As noted earlier, the respondents were largely divided. Those that acknowledged the existence of a mechanism included E2, E3, E9, and E11. Examples of their comments included the following:

- *E2: ADB currently, as part of the banking ecosystem uses a collaborative approach with Ghana Association of Bankers (GAB) to address this.*
- *E3: I will say by law, we are part of the board for NIA. So automatically the platform is there for us to air our views when it comes to evolutions and when it comes to updates.*
- *E9: I believe we have representation on the board and all our view can be channeled through them.*

Those that disagreed such as E1, E6 and E13 also made some comments as follows:

- *E1: No but of course, they can put out questionnaire with vendors or their customers. They can bring out questionnaires on the kind of security we expect them to put in place for us to be comfortable.*
- *E6: For now, No. Nothing. We don't have anything to do with them. We only request. That's all.*
- *E12: So far, I don't think there is. I don't think there's a mechanism except going through the regulator for the financial institutions*.

Finally, some respondents were unsure about the mechanism for the evolution. For instance, E13 stated, "*No idea as I have not read their ISP but I believe we could use the consensus meeting for that*"

ISP Evolution Participants: As noted respondents shared four varied opinions about the participants as below:

First, some respondents believe in delegating a team of internal stakeholders to collaborate with the external stakeholders to review the ISP. An example is where E1 highlighted, "*That should be the task of the security team. They should have a CISO in collaboration with other stakeholders like I.T. So that is their security team, the I.T team and other stakeholders. For instance, their compliance unit. They're also very key*".

Secondly some of the respondents believe that the internal organisation should liaise with the external stakeholders' regulatory organisation. An example is E2 stating, "*It is likely going to be Ghana Association of Bankers (GAB)*".

Thirdly, some respondents believe in bringing all identified external stakeholders together to discuss and review the ISP; such respondents included E1, E3, E4, E5, E8 E9, E10, E11 and E12 and examples of their comments included statements such as:

- *E3: I think that it is both organisations and some individuals. For the organisations, they will be enormous.*
- *E8: All the organisations that are required to use a Ghana card [are to be part]. In fact, the Ghana card now is supposed to be the unique identifier for all individuals transacting anything in Ghana. So in their policies, their amends or whatever should involve all those that are affected. It'll enrich it.*

Finally, some respondents highlighted the need to bring everybody to participate in the review process. E6 for instance states, "*We have a policy, and we have all agreed on that policy; we brought everybody on board and agreed that that is the way to go. We review it annually, which is even bad. Ideally, it should be every quarterly or every half year, but we review it annually. And then everybody signs it. When you are leaving, we have a leaving policy detailing whenever you are leaving, whatever you need to do, whoever is coming in and day-to-day operations within. We have policies because we have a network here. So, there are policies that we follow*".

6.6 Discussion

This section explores the findings on the views, thoughts, and extent of stakeholders' involvement in the development, awareness creation, compliance, enforcement, and evolution processes of the Ghanaian National Identity System (GNIS). These findings are discussed in relation to existing literature on information security (IS) effectiveness, IS management (ISM), and IS policies (ISP).

6.6.1 Information Security Effectiveness

Our study's findings on IS effectiveness align with existing literature in terms of understanding its meaning and implementation. Participants described "information security effectiveness" as encompassing both human and technical activities aimed at protecting or enhancing the security of data, systems, hardware, and networks within organisations, involving various stakeholders.

This understanding is consistent with the literature, where IS effectiveness is achieved through a combination of data security measures, regulatory controls, collaboration, data confidentiality, and both human and technical approaches. These observations resonate with the findings of Bulgurcu et al. (2010), Jai-Yeol (2011), and Raggad (2010), as highlighted in Chapter 5 discussion on IS effectiveness which emphasised the literature recommendation of using multi-faceted approaches to safeguarding organisational data and systems.

Additionally, we noted that Bulgurcu et al. (2010) highlighted the critical issue of compliance and suggested that policy awareness campaigns and education are essential for ensuring IS security within organisations.

Respondents identified several key approaches to enhancing IS effectiveness, including effective data collection, data sharing, resource sharing, compliance enforcement, stakeholder engagement, recruitment, and training. These suggestions are well-supported by the literature (Culot et al., 2021; Chaudhary et al., 2022; Taylor et al., 2020). For instance, Taylor et al. (2020) argue that ensuring users understand their assurance responsibilities and are aware of the risks to their information systems is a key security control.

Additionally, some respondents noted challenges in data sharing with the NIA, indicating a need for the NIA to improve its data-sharing practices to facilitate better collaboration with other organisations. Respondents also emphasised the importance of enforcing policies to ensure compliance and the need for motivation, aligning with existing literature (ISO 27001 – Monitoring Efficacy & Continuous Improvement, 2021; Herath et al., 2022; Jai-Yeol, 2011). Jai-Yeol (2011) for instance, highlights that motivating employees and adopting human-centred measures based on human behaviours can enhance compliance as employees can pose threats through intentional abuse (e.g., data theft, data destruction) or unintentional actions (e.g., forgetting to change a password, forgetting to log off).

Further to the above, respondents believe that involving stakeholders in IS management and improvement can enhance human participation in preventing security breaches. Participants emphasised the need for the NIA to engage more stakeholders to improve IS effectiveness, reflecting literature suggestions (Alshaikh et al., 2022; Jai-Yeol, 2011). Jai-Yeol (2011), which asserts that many organisations underestimate the importance of managing human functions and rely heavily on technological solutions without considering the human aspect of security breaches.

Participants also highlighted the importance of an effective recruitment process and training on key issues such as the Citizenship Act, NIA Regulatory Laws, and Criminal Laws to improve IS effectiveness. This knowledge helps employees make informed decisions regarding registration and compliance.

Finally, respondents identified the need for government involvement, enhanced information privacy, and business continuity to facilitate IS effectiveness and improvement. For instance, some respondents noted that effective security is crucial for guaranteeing business continuity and executing mandates as a government or revenue mobilisation officer.

6.6.2 Information Security Management (ISM)

The findings reaffirm the critical importance of ISM, as emphasised by respondents and supported by existing literature. This is also in line with previous studies on external stakeholders. They believe that the NIA should adopt multi-faceted approaches to ensure ISM aligns with literature recommendations from Halperin & Backhouse (2012); Aichholzer & Strauß (2010); and Saxby (2006). Respondents maintained that confidentiality, integrity, and privacy of data and systems are essential for effective ISM, consistent with Halperin and Backhouse (2012), who identified competence, integrity, and benevolence as dimensions of trustworthiness in government.

The data revealed some confusion regarding the department or unit responsible for ISM. While some respondents believed it was handled internally, others thought it was an external issue. Clarity is needed to ensure organisational sanity, transparency, and accountability, especially as external stakeholders rely on the NIA for data verification, authentication, integration of customer records, data sharing, and collaboration.

EIS organisations in public-private arrangements need to adopt more effective security approaches to avoid system and data compromise. This helps to manage the significant interest, and the primary motive of key responsible officers who are mandated to safeguard government EIS organisations in such arrangements as noted in the study. The insights from the external stakeholders provide useful insights into the strengths and weaknesses of the current NIA information security policy. By addressing these concerns and recommendations, policymakers can enhance the effectiveness of the system, ensuring it meets the needs of all citizens.

The study also revealed new suggestions, such as involving the government in general IS efforts. This aligns with Raggad (2010), who suggested that organisations adopt multi-faceted strategies to manage information security and protect data against attacks using technical, operational, and managerial controls. Finally, respondents also emphasised the need for administrative, organisational, and technical resources to ensure effective ISM for EIS organisations. They believe that the adoption of legal, administrative, human, social, and technological approaches impacts the acceptability and trust issues associated with such systems by addressing concerns about personal data.

6.6.3 Information Security Policy (ISP)

ISPs are essential tools used by governments, organisations, and institutions to protect their information resources, including data and systems. They also help achieve institutional, corporate, regional, and national benefits. This study reinforces previous findings on the use of ISPs, focusing on EIS ISPs. Whitman et al. (2001) explain that ISPs guide employees in ensuring information security to fulfil organisational roles. Compliance with ISPs is considered a critical socio-organisational resource (Boss and Kirsch, 2007; Siponen et al., 2007). Aurigemma and Mattson (2019) suggest that ISP compliance literature should focus on mechanisms, treatments, and behavioural antecedents related to specific threats rather than attempting to cover all security actions.

Organisational practices recommend that employees follow various policies outlined in their organisation's ISP document (Bulgurcu et. al., 2010; Crossler et.al, 2014; Moody et.al, 2018). This study highlights how and why ISPs are used to prevent unauthorised data access and protect individuals' identities, ensuring compliance among employees and stakeholders. The NIA uses ISPs as preventative and mitigating actions against specific threats, as recommended by Siponen & Vance (2014), Siponen & Baskerville (2018), and Aurigemma and Mattson (2019), detailing their resolve to avoid common security violations.

Regarding the challenges in ISP Implementation, the study highlights that despite the NIA's high standards for ISPs, little action has been taken to achieve these standards within the organisation. Clear standards must therefore be set to make EIS ISP provisions more effective. Aurigemma and Mattson (2019) note that compliance with each security action requires different thought processes, time, diligence, knowledge, and effort.

Further to the above, the data shows varied opinions among stakeholders regarding the formulation, development, and management of NIA ISP. Some respondents believed in the existence of an NIA ISP, while others were unsure. This discrepancy is concerning, especially since some user agencies or external stakeholders lack confidence in the status of an important document meant to guide behaviour in preventing, detecting, and responding to security incidents (Cram et al., 2017).

Governments, organisations, and institutions must therefore ensure that employees and stakeholders understand their ISP requirements. Alqahtan (2018) asserts that an ISP bridges the gap between organisational expectations and individual contributions to ISP implementation, which should be clear and understandable. The NIA and other EIS organisations should ensure that the status of their ISPs is known by both internal and external stakeholders. This supports appropriate behaviour by providing clear instructions on responsibilities (Siponen et al., 2014). The NIA must resolve these tensions through effective sensitisation and awareness campaigns, boosting stakeholders' confidence, knowledge, and understanding of the ISP and its status.

On the ISP Awareness, the findings of this research reinforce the importance of prioritising ISP awareness among stakeholders, especially in EIS institutions. This is crucial for ensuring security and addressing trust and privacy concerns related to data handling. The research highlighted various ISP awareness approaches and strategies, such as educating and sensitising stakeholders on data protection rights and privacy, emphasising the importance of employees' roles, and testing stakeholders' understanding of ISP awareness. According to Johnson et al. (2016), most security issues are attributed to employee actions, a persistent problem for organisations (Johnston et al., 2016), as evidenced by incidents at Morgan Stanley and Gillette (Schmerken, 2015). Siponen (2006), Spears & Barki (2010), and Wiant (2005) acknowledged that the reputational, financial, and legal implications of information security incidents have led many organisations to develop and implement ISPs to create awareness on topics such as access controls, data classification, data storage, and virus protection. Scholars like Guo (2013), Karlsson et al. (2015), Lebek et al. (2014), and Taylor et. al., (2020) have extensively written on employees' security awareness, culture, and compliance issues in organisations. For instance, Taylor et al., (2020) highlighted that a part of creating and managing the organisational culture is through the development of an ongoing security awareness programme that focuses on training, awareness of laws and industry regulations during inductions to ensure that the employees develop a positive attitude.

Additionally, the study noted that some respondents lacked adequate knowledge about the NIA ISP. The research therefore recommended strategies such as education and sensitisation on data protection rights and privacy, emphasising employees' roles, and testing stakeholders' understanding of ISP awareness. This aligns with best practices in the literature. For instance, Alassaf and Alkhalifah (2021) stress the need for employee ISP awareness and compliance, echoed by stakeholders' calls for better awareness and training. It is crucial for EIS organisations to have an ISP that addresses external stakeholders' needs and contributions to ensuring the security of the organisation's information resources.

On the ISP Content, external stakeholders highlighted the need for NIA and EIS organisations to focus on critical approaches and strategies covering network security, personnel security, software security, policy management, data sharing, general security management, access rules, and employee conduct. The study emphasised that EIS organisations must include physical security, application security, data life cycle management, employee education, legal and statutory requirements, and business continuity plans in their ISP content to protect their information resources adequately. These aspects are well-documented in the literature (Culot et al., 2021; Taylor et. al., 2020; Chaudhary et al., 2022). On Business continuity, for instance, Taylor et al., (2020) argue that it is critical and should be part of the mechanisms of any organisation to allow continuous operations and should involve a number of key personnel as participants in a workshop and and their various responsibilities clarified to them.

The study also highlighted the need for clarity in ISP content to ensure easy understanding by employees. This aligns with findings by Goel and Chengalur-Smith (2010) and Pathari & Sonar (2012), who believe that ISP content needs to be concise and easy to understand. For instance, the breadth, clarity, and brevity of the document are important for reader comprehension (Goel and Chengalur-Smith, 2010). Lopes and Sá-Soares (2010) argue that unclear ISP content can inhibit policy adoption. Niemimaa and Niemimaa (2017) note that an ISP is a “dead object” unless materialised in the actions of its subjects.

Respondents also identified the need to factor in the organisation’s IT infrastructure, environment, and business continuity interests as part of the ISP content. This aligns with findings by Hong et al. (2006), Karyda et al. (2005), Knapp et al. (2009), Warman (1992), and Wall (2013), who explain that internal and external factors can pose potential risks to an organisation, necessitating preventive measures.

The study also notes that organisations must include guidelines, regulations, and standards to protect data-sharing specifications and employees’ acceptable conduct. This aligns with arguments by Knapp et al. (2009), Siponen (2006), and von Solms (1999), who emphasise the importance of ISPS complying with recommended external security standards, guidelines, and regulations such as NIST, ISO27001/2, COBIT, HIPAA, and PCI DSS. For instance, Siponen and Kinnunen (2018) note that the ISO27002 standard recommends several areas of content, including management direction and cryptographic control (ISO/IEC 27002, 2013).

Respondents identified factors that fall within the seven factors identified by Karyda et al. (2005), including organisational structure, culture, management support, contribution to users' goals, security offices, user participation in the formulation process, training, and education. These factors relate to ISP content and method in various ways; for example, a security-ignorant organisational culture may necessitate a new cycle in ISP development (Talbot and Woodward, 2009). However, Baskerville & Siponen (2002) acknowledged that organisations have different needs, and the same general policy recommendations cannot apply to all organisations. EIS organisations should acknowledge their internal and external security needs to create adequate policy content addressing their challenges.

The study reinforces the need for EIS organisations to include general security management strategies in their ISP content, such as data backup, employee user access for stakeholders' data exchange, transition, and redundancy. Baskerville et al. (2014) and Siponen and Iivari (2006) note that organisations in volatile markets, such as EIS markets, require adaptable guiding principles and recovery plans.

Regarding ISP Governance, the research highlights the importance of ensuring awareness and strict adherence to the ISP governance framework in EIS organisations to prevent confusion, such as some respondents being unaware of the effectiveness of the NIA ISP governance process. Ensuring awareness and compliance by stakeholders would adequately cater to the organisation's information environment and security needs, especially considering that the human aspects of information security should be considered in addition to the technological aspects (Furnell et al., 2016). Furnell et al. (2016) argue that the absence or inadequate information security awareness, ignorance, negligence, apathy, mischief, and resistance cause users' to make mistakes and that effective ISP governance and compliance with organisational information security policies mitigate the risk of employees' behaviour.

Additionally, respondents generally believe that the NIA should have an effective ISP governance process to ensure IT infrastructural security and effectiveness. As Alqahtani (2017) noted, such provisions provide clearer and practical steps necessary to help orrganisations to improve their is programmes. These observations help organisations determine if changes in organisational structure or procedures influence the effectiveness of their ISPs (Yin, 2013). An effective governance plan should clearly outline the objectives, extent of involvement, participants, requirements, and procedures that the EIS organisation must use.

Regarding the ISP Development Process, the study shows the need for EIS institutions and organisations to develop their own ISPs to enhance acceptance and effectiveness. Respondents believe that internal and external stakeholders should be involved in the ISP development process due to their influence and roles in protecting the system and data. This aligns with literature suggesting that an organisation's security culture can affect the ISP, making user participation in the ISP development process advisable (Da Veiga and Eloff, 2010). Colwill (2009) argues that internal stakeholders can be a significant resource or risk to information assets, hence their participation in the ISP development process is often recommended.

The study also identified formal and informal stakeholders that should be involved, including telecommunications networks, banks, security services, revenue mobilisation institutions, and other service providers. This is similar to Maynard et al. (2011), who argue that stakeholder groups in ISP development could include business units, executive management, human resources, IT departments, legal advisors, and public relations. Managers play a key role in ISP development and implementation, aligning the ISP with business processes (Soomro et al., 2016).

The research highlights that EIS institutions and organisations should involve all relevant stakeholders in the development process. Coles-Kemp (2009) and Lapke and Dhillon (2008) argue that selecting relevant stakeholders for ISP development may require its own method, and disregarding the context of an ISP during development can lead to implementation and compliance issues (Chen et al., 2012).

A unique finding is that government-financed EIS organisations should recognise applicable legal requirements and factor them into the ISP development process. Organisations should involve named stakeholders in the development process while avoiding excessive political interference, which can compromise system and data security.

Respondents also emphasised the need for clarity and transparency in the NIA ISP. The NIA should be more transparent about how external stakeholders can be involved in the development, management, and implementation of the ISP.

On the ISP Development Mechanisms, the study identified concerning trend of respondents highlighting the absence of ISP development mechanisms. This underscores the urgency for

EIS institutions and organisations like NIA to clarify, identify, involve, and educate all stakeholders on the mechanisms available for participating in the ISP development process.

Regarding ISP Enforcement, the research findings reinforce some of the findings by other scholars and provide key considerations for EIS institutions and organisations. While the NIA ensures employees' compliance and general ISP enforcement through compliance monitoring and awareness creation, there are recommendations to facilitate internal and external ISP enforcement and implementation. This may be partly due to a lack of adequate compliance awareness through training and sensitisation or the absence of clear instructions in the ISP about employees' and user agencies' compliance enforcement responsibilities. According to Siponen et al. (2014), ISPs support appropriate behaviour among employees by providing clear instructions on responsibilities. Flowerday and Tuyikeze (2016) argue that employees who comply with the organisation's ISP are assets to organisational security. Alqahtani (2017) emphasises that introducing ISPs to all stakeholders, including end-users, is essential for ensuring compliant behaviour. Including different representatives may benefit the implementation phase if they act as ISP advocates (Maynard et al., 2011; Rees et al., 2003).

The study also observed that members of the NIA Board of Governors have more influence in the policy process than other institutional stakeholders. Respondents emphasised the need for Board representatives to explain the NIA ISP and the importance of compliance to their organisational staff.

Regarding Compliance Awareness and Employee ISP Compliance, the research highlights the significant impact of compliance awareness on employee ISP compliance, especially in EIS organisations. It underscores the necessity for EIS organisations like the NIA to ensure that all stakeholders, both internal and external, are aware of, understand, and comply with the NIA ISP. This aligns with Knapp & Ferrante's (2012) findings, which show a positive relationship between policy awareness, enforcement, and policy effectiveness. The study's findings are also consistent with ISO 27001 guidelines and the work of Herath et al. (2022) and Jai-Yeol (2011), who advocate for human-centred measures to enhance compliance as noted in the Chapter 5 discussion section 2.

On the ISP Evolution, the study highlights the importance of regular review and updates of the NIA ISP, emphasising the involvement and influence of participants in ensuring data and system security. This aligns with the literature, which shows that organisations regularly update their ISPs to meet organisational needs and protect assets. The IS control literature highlights the importance of policy evolution as a means for organisational management to identify and correct existing problems (Choudhury and Sabherwal, 2003; Cram et al., 2016a). Cram et al. (2017) noted that employees might exhibit increased compliance with the deployment of a new, more rigorous policy. This reinforces findings by Knapp & Ferrante (2012) and Doherty & Fulford (2005), who identified that policies are updated based on age, policy scope, and best practices.

Additionally, the study highlighted that stakeholders expect their views to be considered and to influence the NIA ISP through policy inputs, feedback, and implementation support during the evolution process. EIS organisations should ensure policy evolution training, stakeholder monitoring, and external enforcement to protect data and systems. This aligns with Cram et al. (2017), who found that aspects of policy training, implementation, monitoring, and enforcement contribute to identifying opportunities for policy improvement. Rees et al. (2003) noted that ISP evolution includes four core life cycle steps: plan (development, definition), deliver (implementation), operation (review trends, monitor operations), and assessment (policy assessment, risk assessment).

Respondents further indicated the need to recognise legal and regulatory guidelines, liaise with regulatory stakeholder organisations, and consider environmental, social, and technological factors when reviewing the organisational ISP. This is particularly important for government-controlled EIS systems, which require a stringent review process, including central government approval. The NIA, being government-controlled with private company involvement, requires a complex evolution process and governance system. Cram et al. (2017) noted that a more complex system of governance is needed to effectively oversee, monitor, review, update, and approve policies.

Regarding the mechanisms for the evolution process, respondents were divided on the existence of mechanisms for influencing or participating in the evolution process. This division may be due to the government's decision to recognise some organisations as formal stakeholders while others are considered non-formalised stakeholders. Formal stakeholders have legal representation on the NIA Board and are required to participate in ISP discussions, evolution, and approvals. The study noted that these formalised organisations have more insights about the NIA ISP than the non-formalised organisations. To address this, non-formalised organisations should be given more active roles during the evolution and development process of the NIA ISP. Additionally, there should be enhanced mechanisms for stakeholders, including regulatory bodies and the NIA, to collaborate more effectively during the evolution phase of the NIA ISP.

6.7 Concluding Remarks

The chapter discussed the aims and objectives, study design, procedures, analysis, and results of the third study, which focused on the formal and non-formalised external stakeholders' views about the NIA's IS effectiveness, IS management, and ISP.

The study discussed formal and informal external stakeholders' perceptions of the NIA ISP and its formulation, enactment, development, and evolution processes. It also analysed their responses to their ISP regarding their involvement, governance effectiveness, evolution process, compliance, and awareness. The research also assessed the effectiveness of the NIA ISP, its content, importance, enforcement, and the status of the policy from the external stakeholders' perspective.

From the study, the researcher notes that the NIA Information Security Policies (ISP) are perceived as generally effective in protecting its identity system by respondents and meet the high standards required in the literature. However, there is little attention and clarity on implementation measures to be used in achieving their organisational ISP objectives. The study also highlights the conflicting views of respondents on whether or not an ISP is a technical or non-technical document to the NIA and the varied opinions on who is responsible for ISP management.

The next chapter focuses on the study conducted on the General Public's involvement in the formulation, development, and implementation processes.

7 Study 4 on General Public Survey

The previous chapter discussed user agencies' views and perceptions about their involvement in the NIA ISP development, enactment, and evolution process as external stakeholders. This chapter focuses on the views and perceptions of the general public as external stakeholders in the policy development, evolution and implementation processes of the NIA. The chapter also analyses the involvement of members of the public as external stakeholders of the National Identification Authority (NIA) in their policy development, evolution and implementation processes. The chapter also analyses the trust levels of the public in NIA and its staff to gain a more specific understanding of trust in specific government services or organisations and its staff.

In a broader perspective, the chapter highlights the important considerations for electronic identity systems (EIS) to contribute to the ISP development and evolution processes and ensure the practicability of the recommendations made from the study.

To do this, we begin the chapter with the study design section, then the participants and study procedures section, then focus on the data analysis and the study results. The chapter then concludes by making some recommendations on the members of the public's involvement in the ISP development processes and how to enhance the methods to achieve both organisational objectives and public trust.

7.1 Study Design

As noted in Chapter 3, this study's research objectives include:

- To investigate the public's perceptions and views about the formation, expression, and evolution of the National Identification Authority Information Security Policy (NIA ISP).
- To understand the perception, expectations and public beliefs about NIA's Information Security Policy (ISP) and trust issues that the users/the public have towards the NIA and its employees.
- To determine how the public trusts the NIA's Information Security Policy (ISP) enforcement process and the challenges encountered during compliance.

As noted in Chapter 3, to achieve the above objectives, we designed a questionnaire (see details in appendix 9.8) with adapted questions from authors to elicit responses from the public on the perceptions, views and expectations of the respondents' ISP awareness, importance, beliefs and trust using a 7-point Likert scale.

These questions were adapted to be in line with our research objectives relative to the particular themes under consideration. To understand the public's perceptions about formation, expression, and evolution, for instance, we adapted tested questions from Flowerday and Tuyikeze (2016). On the public trust for both the NIA and its staff, we adapted the questions from McKnight et al. (2002), while on the public communication, we adapted questions from Flowerday and Tuyikeze (2016) and Adele Da Veiga (2018) as detailed below:

Theme	Adopted Author/Source	Question
Public expectations	Flowerday and Tuyikeze (2016)	It is important that the NIA explain to the public for which purposes their personal information will be used. It is important that the NIA explains to the public how their personal information will be secured. It is important that the NIA explains to the public how their personal information is secured when shared with other organisations (government organisations, banks, telecoms). It is important that the public is involved in the development of the NIA ISP. It is important that the public is consulted for any amendments of the NIA ISP. It is important that the NIA ensures its staff are aware of the provisions of its ISP. It is important that the NIA ensures its staff comply with the provisions of its ISP.
Public communication	Flowerday and Tuyikeze (2016) and Adele Da Veiga 2018	The NIA has explained to the public for which purposes their personal information will be used. The NIA has explained to the public how it ensures that their personal information cannot be accessed by unauthorised parties.

		The NIA has explained to the public how it ensures that their personal information cannot be modified by unauthorised parties. The NIA has explained to the public how it ensures that their personal information is available for authorised parties to use. The NIA has explained to the public how it ensures that their personal information is protected when shared with other organisations (government organisations, banks, telecoms). The NIA informs the public in a timely manner as to how information security changes will affect the security of their personal information.
NIA Trust	McKnight et al., 2002	Competence (McKnight et al., 2002) The NIA is effective in protecting citizen personal information. The NIA is skilful in protecting citizen personal information. The NIA is very knowledgeable about information security. The NIA performs its role of protecting citizen personal information very well. Benevolence (McKnight et al., 2002)

		If citizens need help in protecting their personal information, the NIA will do its best to help them. I believe the NIA acts in the best interest of citizens when managing their personal information. The NIA is interested in the wellbeing of citizens when managing their personal information. Integrity (McKnight et al., 2002) The NIA is truthful in its dealings with citizens about the handling of their personal information. The NIA is sincere with citizens about the handling of their personal information. The NIA keeps its commitments to protect citizen personal information. The NIA is honest about the handling of citizen personal information.
NIA Public involvement – ISP development & evolution		The NIA has involved the public in the development of its ISP. The NIA consults the public for any amendments to its ISP.

NIA Staff Trust	McKnight et al., 2002	Competence (McKnight et al., 2002) NIA employees are effective in protecting my personal information. NIA employees are skilful in protecting my personal information. NIA employees are very knowledgeable about information security. NIA employees perform their role of protecting my personal information very well. Benevolence (McKnight et al., 2002) If I need help in protecting my personal information, NIA employees will do their best to help me. I believe NIA employees act in my best interest when managing my personal information. NIA employees are interested in my wellbeing when managing my personal information. Integrity (McKnight et al., 2002) NIA employees are truthful in their dealings with me about the handling of my personal information. NIA employees are sincere with me about the handling of my personal information. NIA employees keep their commitments to protect my personal information.

		NIA employees are honest about the handling of my personal information.

Table 15: Adapted Questions and their Sources

We developed our own questions for NIA Public involvement in ISP development and evolution. This is due to the absence of existing questions in the literature that deal with the aspect of public involvement that we researched.

7.2 Participants and Procedures

7.2.1 Participants

As noted in Chapter 3, this study involved distributing 200 paper Questionnaires to the public throughout the four NIA operational regions using a distribution formula primarily developed based on the country's regional population distribution. We administered the questionnaire to the public on 10 January 2022 and 17 February 2022.

We received 155 responses from participants. Out of the 155, we excluded seventeen (17) responses during the data quality checks and analysis because they were incomplete. We manually collected the results of the self-administered questionnaire, which were later entered into Qualtrics for ease of analysis. The manual data collection ensured easy access to participants and prevented the impact of the unstable internet connectivity in the regions we collected the data from. This means that the final study analysis for this study focused on 138 responses. All participants were over 18 and consented to participate in the study.

7.2.2 Procedures

As noted in the study procedure section (section 3.11) in Chapter 3, we obtained ethics approval from the Computer and Information Science Department’s Ethics Committee (see details in appendix 9.2, and 9.7). We then conducted a pilot study with 10 Ghanaian research students at the University of Strathclyde and used the feedback to improve the study design for the primary data collection exercise. The pilot study feedback was largely typographical errors, and we corrected them.

The study adapted questions and we also developed our own questions. The adapted questions and our developed ones are crucial in helping us to understand public expectations relative to the security of their personal and sensitive data held by organisations. This is due to the public’s interest for organisations to have robust and effective information security policies in place to protect their data from misuse. Therefore, understanding the processes involved in developing such policies is key to meeting these public expectations.

Regarding the demographic questions, the questionnaire covered three (3) demographic questions that included the Gender, Age range, and highest educational level of respondents, while the rest of the thirty-seven (37) questions were for Non-demographic data.

7.3 Analysis

We first entered the data of the paper questionnaires into Qualtrics.

As noted in the Chapter 3, before the analysis, we examined the dataset for its quality to ensure that only attentive responses and those representative of standard answers were retained. We did this by reviewing and verifying all responses. As noted in the study design section in Chapter 3, we also used methods for identifying careless responses (Meade & Craig, 2012) to filter out participants who may not be paying attention. We used red herring questions (what is your favourite football club?) and participant’s response times to identify the careless responses. We then reviewed and verified all responses and imported and stored the data into the Statistical Package for Social Science (SPSS) software to sort the data into smaller units or groups such as public communication, trust-related groups, etc, as Janssens et al. (2008) recommended for further analysis of the 138 responses after assigning participants with unique identifiers between 1 and 138.

7.4 Results

The study results were further analysed under the Demographics and Non-Demographics.

7.4.1 Demographic

Under the demographic results, we analysed respondents' data such as their gender, age and level of education of respondents. The details are as presented below:

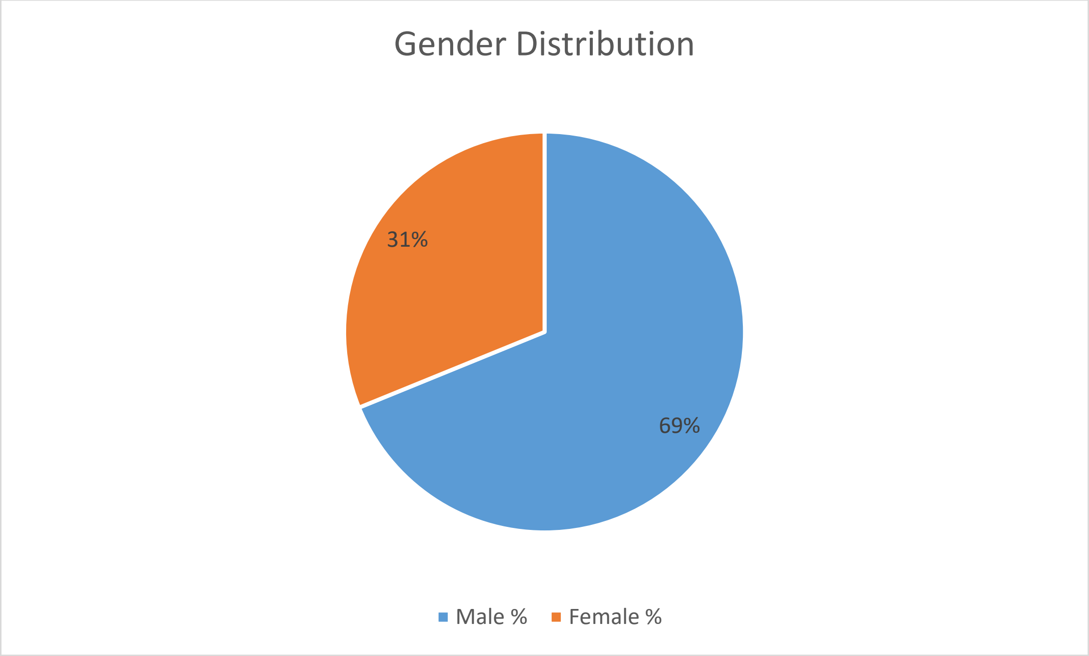


Figure 23: Gender Distribution

On gender results, the data indicated by Fig 23 that there were twice as many male respondents as female respondents, with a male sample of 69% (95) compared to a female sample of 31% (43). This significantly does not reflect the national population distribution, where females constitute 50.7% and males 49.3%. This discrepancy indicates a significant bias in the sample for literate persons and could be attributed to the nature of selecting the participants, and the channels used for recruitment. However, it is widely accepted that literate participants are more likely to comprehend the consent forms and the implications of their participation as well as ensuring that ethical standards are upheld. Literate persons also ensure that the data collected is reliable, and the research process is feasible.

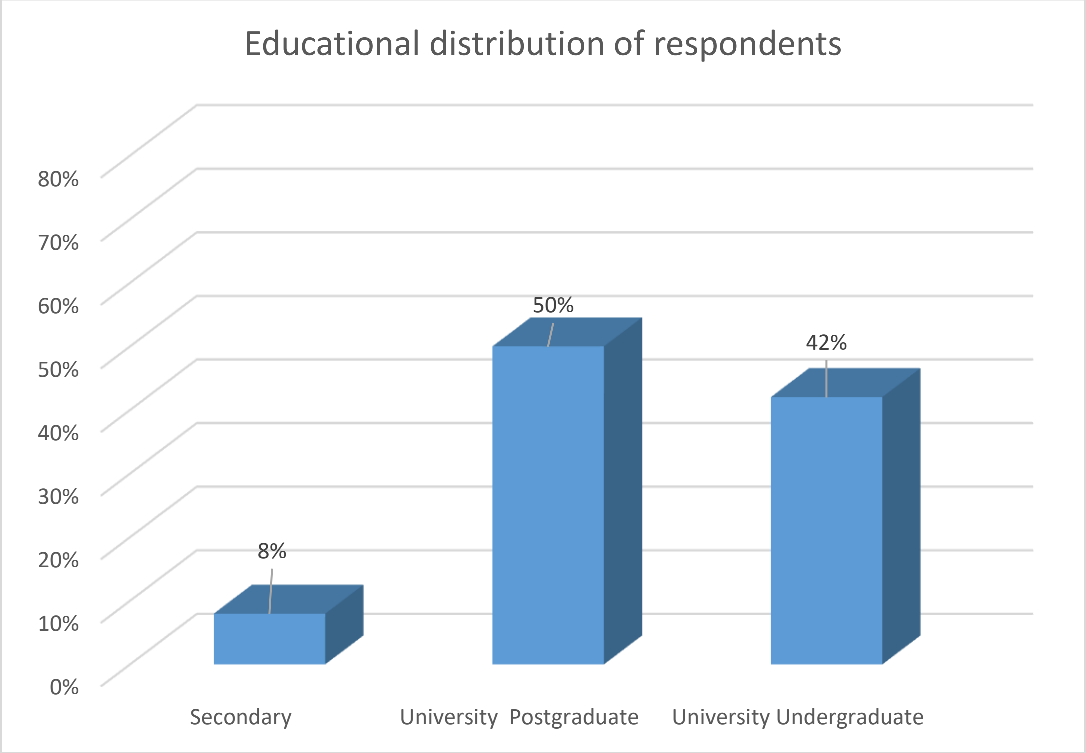


Figure 24: Gender vs Educational background of Respondents

From Fig 24, the data shows that the majority of respondents had a university postgraduate education, constituting 50% (69) of the entire sample. This was followed by university undergraduates at 42% (58) and those with a secondary school education at 8% (11). The educational breakdown across all participants is as follows:

- Secondary School: 8% (11)
- University Undergraduate: 42% (58)
- University Postgraduate: 50% (69)

This distribution indicates a significant bias towards literate individuals, with no illiterate respondents included, even though illiterate individuals comprise over 30% of the population based on the 2021 census. Additionally, the sample has a higher proportion of university graduates and postgraduates compared to the general literate population. This largely reflects the situation in Ghana where the National literacy per the 2021 Population and Housing Census is 69.8%. The 2021 Population and Housing Census in Ghana shows that 40.7% of the population aged 18 years and above attending school are at the tertiary level. Additionally, the census figures highlight that 13% of those who had attended school in the past had tertiary education as their highest level. This indicates that a significant portion of the literate population in Ghana has had a university degree or higher.

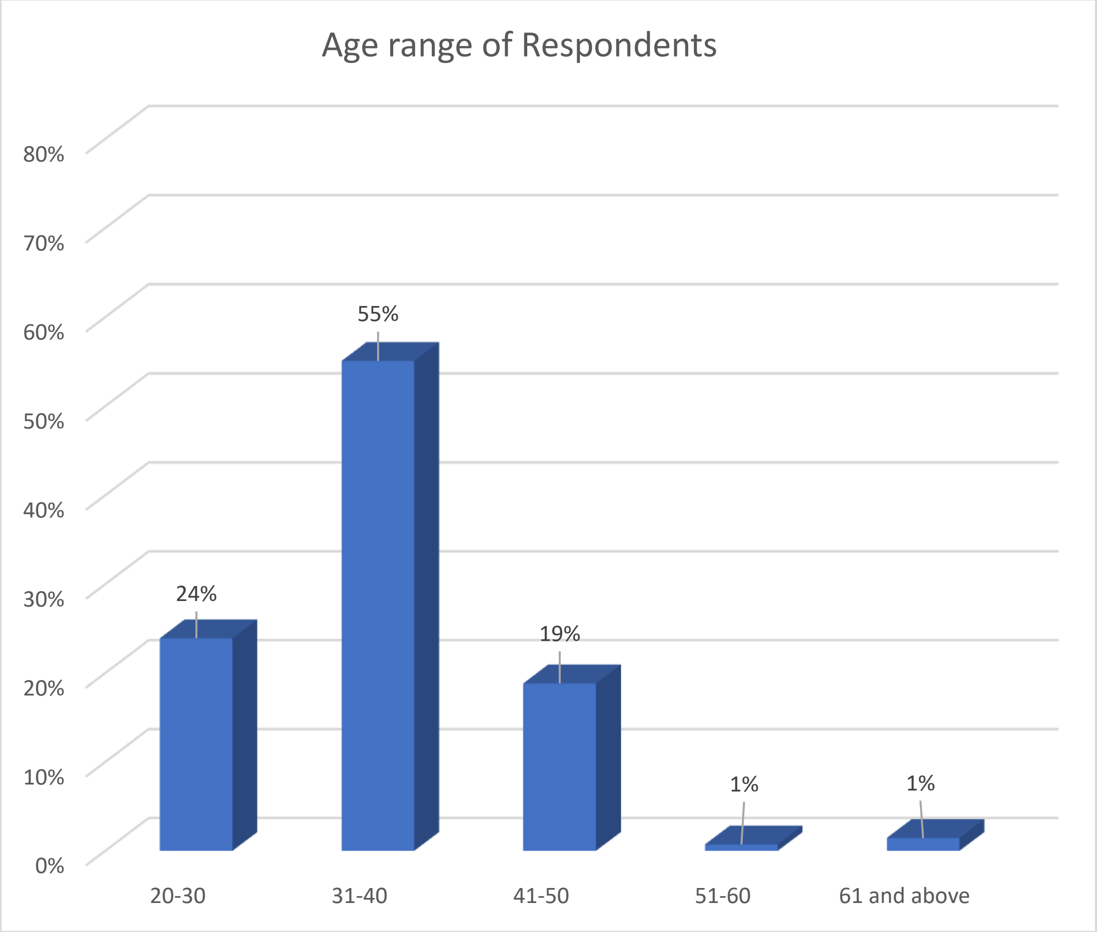


Figure 25: Age of Respondents

In terms of age range, the majority of respondents (55%, 76) were aged between 31 and 40 years. This was followed by 24% (33) aged between 20-30 years, 19% (26) aged between 41-50 years, 1% (1) aged between 51-60 years, and 1% (2) aged above 60 years. This age distribution suggests an overrepresentation of older individuals compared to the national population, where the majority are young people aged 15-35 years from the 2021 National Population and Housing Census. This obviously could be attributed to the fact that the study only focused on individuals over the age of 18 for ethical reasons.

7.4.2 Non- Demographic Results

Under the non-demographic questions, we examine the reliability of the scale used for the questions. The analysis of the questions was done in groups in the following order:

- Public Expectation

- Public Communication
- NIA Trust
- Public Involvement in ISP Development and Evolution
- NIA Staff Trust

7.4.3 Scale Reliability

As noted in Chapter 3, we evaluated the scale's reliability using the Cronbach alpha under the study procedure. We evaluated the ISP Questions under the five main themes or groups for their consistency, and the results are as presented below:

Summary of the Cronbach Alpha

Themes	Sub-themes	Cronbach Alpha	No. of Items
Public Expectation		0.804	7
Public Communication		0.937	6
NIA Trust	Competence	0.924	4
	Benevolence	0.910	3
	Integrity	0.958	4
Public Involvement ISP Development and Evolution		0.928	2
NIA Staff Trust	Competence	0.960	4
	Benevolence	0.944	3
	Integrity	0.968	4

Table 16: Themes and Reliability of Scale

Table 15 above shows that the results have an acceptable reliability with Cronbach's Alpha above 0.6 for all the scales. We therefore included all in our analysis.

7.4.3.1 Public Expectations

On the NIA ISP expectations, we categorised the data into three:

1. Public Expectations on Personal Information Handling
2. Public Involvement in the NIA ISP Process
3. Public Expectations on NIA Staff Awareness and Compliance

Public Expectations Personal Information Handling

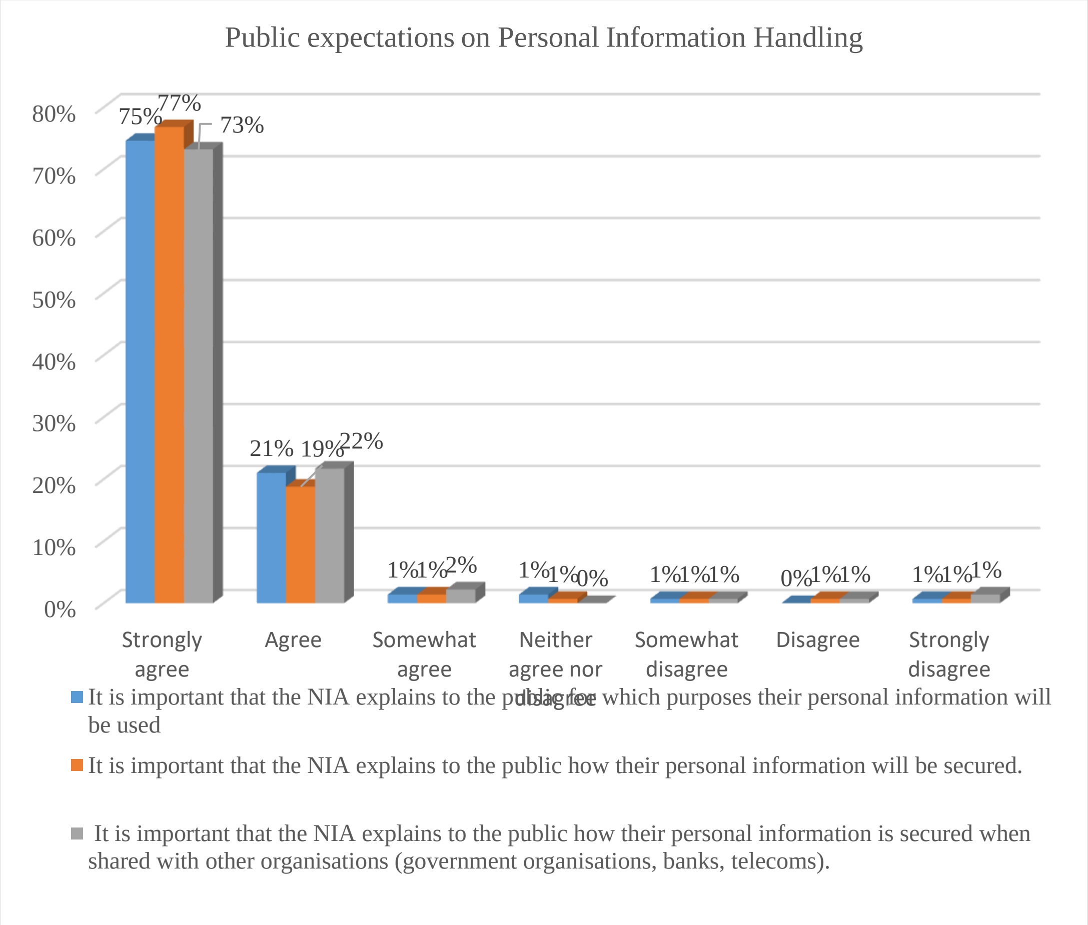


Figure 26: Public Expectations Personal Information Handling Distribution

From Figure 26, it is clear that the overwhelming majority of the public believes and expects that it is important for the NIA to explain the purposes, use, and security of their personal information. Specifically, 97% (133) of respondents cumulatively agree (somewhat agree, agree, and strongly agree) with the expectation on purposes, use, and security of their personal information.

Public Expectations on Public Involvement in the NIA ISP Process

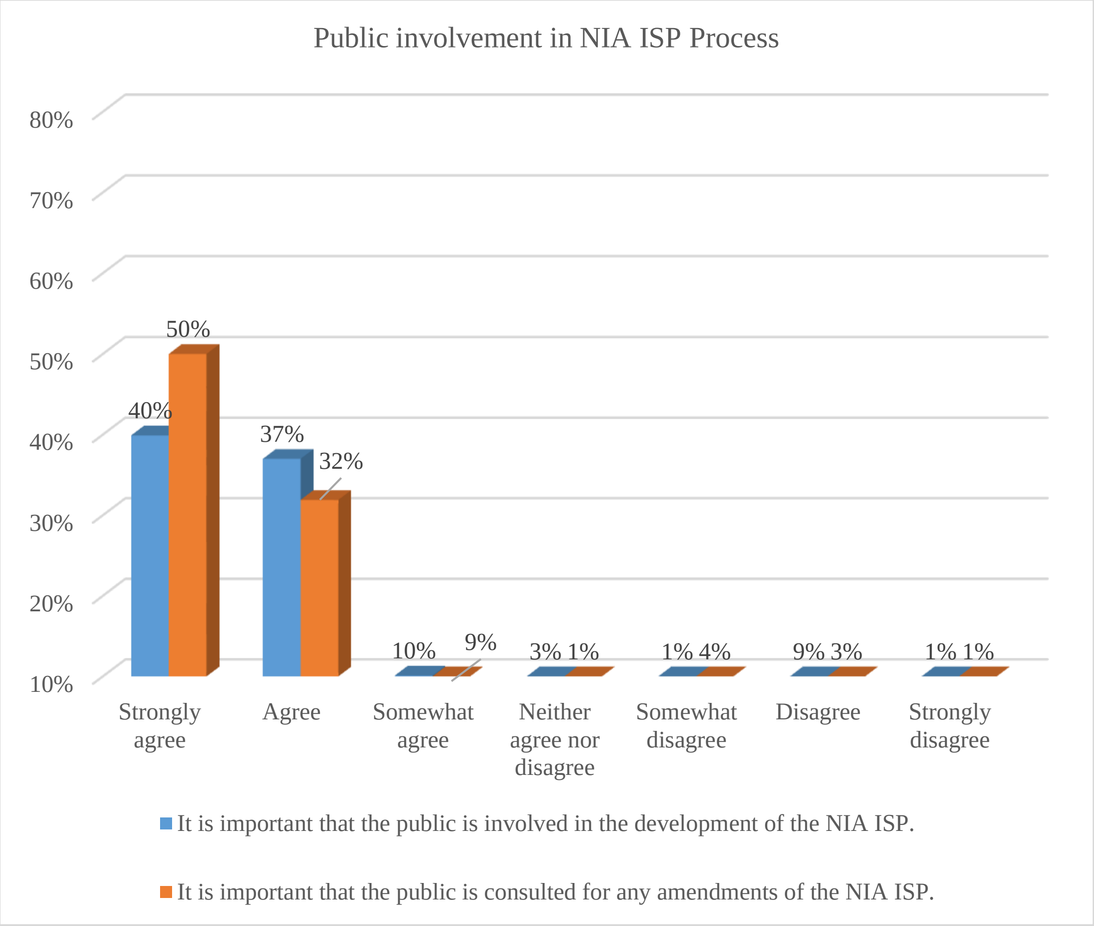


Figure 27: Public Involvement in the NIA ISP Process Distribution

From Figure 27, most members of the public believe and expect the NIA to involve them in the development and revision of the NIA ISP. Specifically, 87% (120) and 91% (125) of respondents cumulatively agree with this expectation on development involvement and amendment consultation respectively, while 11% (14) and 8% (11) respectively disagree. This indicates a strong expectation for public involvement, although a notable minority does not share this view.

Public Expectations on NIA Staff Awareness and Compliance

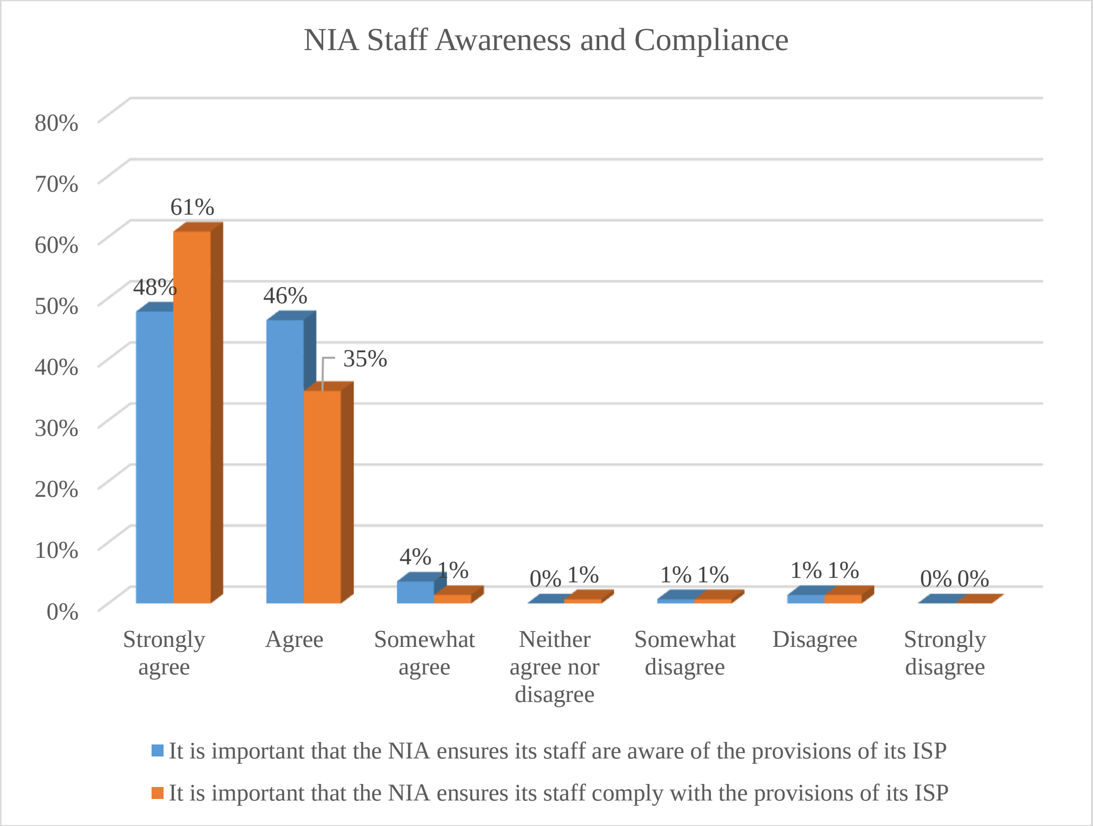


Figure 28: NIA Staff Awareness and Compliance Distribution

From 28, the data shows that 98% (135) and 97% (133) of respondents cumulatively agree that it is important for the NIA to ensure that their staff are aware of and comply respectively with the NIA ISP. This highlights a strong public expectation for staff awareness and compliance with information security policies.

Gender Distribution on Public Expectations

To understand the differences in expectations based on gender, we analysed the responses of male and female participants separately. This analysis helps to identify any gender-specific trends or biases in public expectations (see Appendix 9.10, Figures 39, 40 and 41).

The Public expectations responses based on their gender indicates that both the males and females are cumulatively positive (97% for each), with the males being more strongly positive in their responses than their female counterparts on the purpose of the use of their personal information (79% vs 65%).

On how their personal information is used, both the males and females cumulatively agree on the importance of NIA explaining it to them (96% for males and 100% for females). This means that the females are more positive than their male counterparts. However, the males are more confident in their responses than their female counterparts (72% vs 79%).

Regarding the security of personal information when shared with other organisations, 95% of the females cumulatively agree, while 98% of the males cumulatively agree. The males more strongly agreed than their female counterparts (77% vs 65%).

The males were comparatively more strongly in favour of their responses (41% vs 37%) on the NIA explaining to the public the importance of involving them in developing the NIA ISP. Cumulatively, 91% of the females and 86% of the males agreed. This means the females agreed cumulatively more than their male counterparts despite their lower responses.

On the importance of public consultation for NIA ISP amendments, the females were comparatively stronger in their responses than their male counterparts (65% vs 43%). Again, 96% of the females and 90% of the males cumulatively agreed on the importance of public consultation for NIA ISP amendments. This means that the females responded more positively and stronger than the males.

On the importance of NIA ensuring that members of the public are aware of the NIA ISP provisions, the male respondents were more confident than their female counterparts (40% for females vs 52% for males). Cumulatively, however, both the male and female public members were equally positive in their agreement on the need for NIA to ensure its staff awareness of their ISP (98% for both males and females).

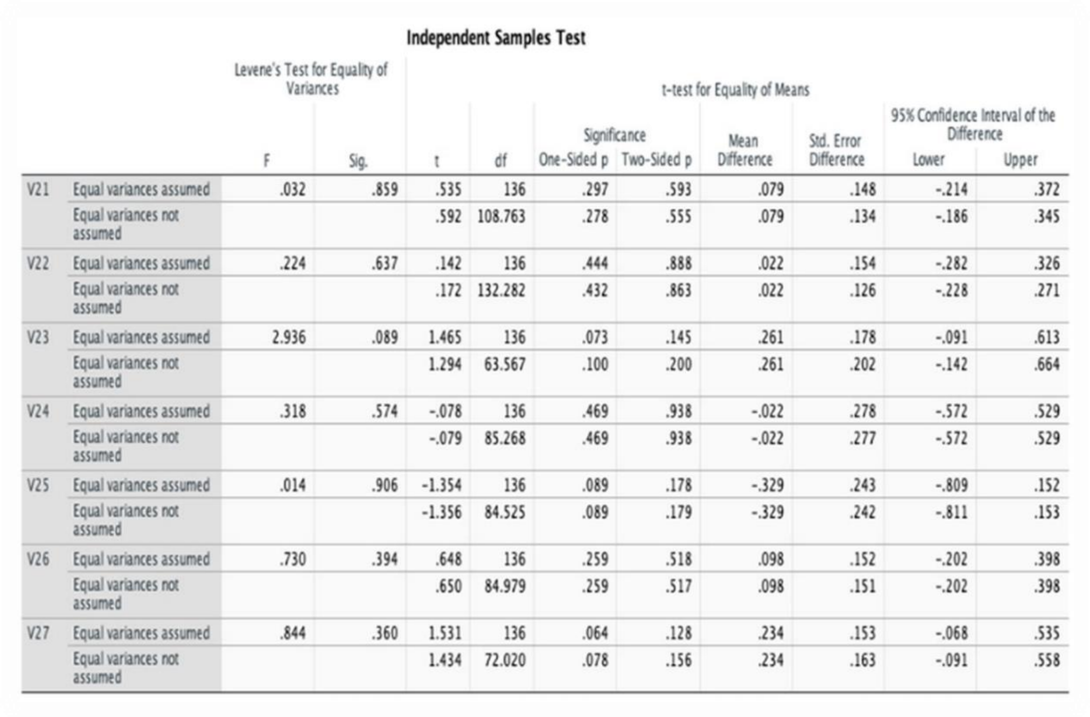
The male respondent members of the public in the study were more decisive in their responses to the importance of NIA ensuring that its staff comply with the provisions of their ISP (66% for males versus 49% for females). Furthermore, 97% of the males agreed with the importance of NIA ensuring compliance with their ISP provisions, while 91% of the females agreed with that assertion. This means that the males were more confident and positive than their female counterparts in their answers.

Question	**Gender**	**Mean**	**Std. Deviation**
It is important that the NIA explains to the public for which purposes their personal information will be used	Female	1.41	0.658
	Male	1.33	0.872
It is important that the NIA explains to the public how their personal information will be secured	Female	1.34	0.526
	Male	1.32	0.953
It is important that the NIA explains to the public how their personal information is secured when shared with other organisations (government organisations, banks, telecoms).	Female	1.59	1.207
	Male	1.33	0.847
It is important that the public is involved in the development of the NIA ISP.	Female	2.16	1.509
	Male	2.18	1.531
It is important that the public is consulted for any amendments of the NIA ISP.	Female	1.68	1.325
	Male	2.01	1.332
It is important that the NIA ensures its staff are aware of the provisions of its ISP.	Female	1.70	0.823
	Male	1.61	0.832
It is important that the NIA ensures its staff comply with the provisions of its ISP.	Female	1.66	0.939
	Male	1.43	0.783

Table 17: Means and Standard Deviation of Gender Distribution

Table 16 above shows the difference in the mean responses of the female and their male counterparts on the public expectation questions. Despite the differences in means, the responses of male and female participants are not very different. This is confirmed by the t-test results, which show no statistical significance between the male and female responses

as presented below:



Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means							
						Significance				95% Confidence Interval of the Difference	
		F	Sig.	t	df	One-Sided p	Two-Sided p	Mean Difference	Std. Error Difference	Lower	Upper
V21	Equal variances assumed	.032	.859	.535	136	.297	.593	.079	.148	-.214	.372
	Equal variances not assumed			.592	108.763	.278	.555	.079	.134	-.186	.345
V22	Equal variances assumed	.224	.637	.142	136	.444	.888	.022	.154	-.282	.326
	Equal variances not assumed			.172	132.282	.432	.863	.022	.126	-.228	.271
V23	Equal variances assumed	2.936	.089	1.465	136	.073	.145	.261	.178	-.091	.613
	Equal variances not assumed			1.294	63.567	.100	.200	.261	.202	-.142	.664
V24	Equal variances assumed	.318	.574	-.078	136	.469	.938	-.022	.278	-.572	.529
	Equal variances not assumed			-.079	85.268	.469	.938	-.022	.277	-.572	.529
V25	Equal variances assumed	.014	.906	-1.354	136	.089	.178	-.329	.243	-.809	.152
	Equal variances not assumed			-1.356	84.525	.089	.179	-.329	.242	-.811	.153
V26	Equal variances assumed	.730	.394	.648	136	.259	.518	.098	.152	-.202	.398
	Equal variances not assumed			.650	84.979	.259	.517	.098	.151	-.202	.398
V27	Equal variances assumed	.844	.360	1.531	136	.064	.128	.234	.153	-.068	.535
	Equal variances not assumed			1.434	72.020	.078	.156	.234	.163	-.091	.558

Figure 29: T-Test Results for Public Expectation

From the t-test results, the data showed no statistical significance between the male and female responses, indicating that gender does not significantly influence public expectations regarding the NIA's handling of personal information, public involvement in the ISP process, and staff awareness and compliance.

7.4.3.2 Public Communication

The Figure 30 below indicates that most public members believe the NIA has explained the purpose of collecting their personal information (70%, 195), how unauthorised persons cannot access their personal information (61%, 84), and how the NIA prevents modification by unauthorised parties (62%, 86). Respondents also believe the NIA has explained how their personal information is available to authorised parties (61%, 84), how it is protected when shared (61%, 84), and how the NIA informs them in a timely manner about information security changes (53%, 73). Despite the majority position, a substantial minority disagrees, and some respondents remain neutral. From the table, 7% (10) were neutral on the purpose of collecting their personal information, 6% (8) of the respondents remained neutral on unauthorised people's access personal information, and 7% (10) were neutral on NIA preventing modification from unauthorised parties. Further, 6% (8) were neutral on personal data being available to authorised parties to use, 5% (7) on the protection of their personal information when shared and 7% (10) in a timely manner the NIA informs them in the event of information security changes.

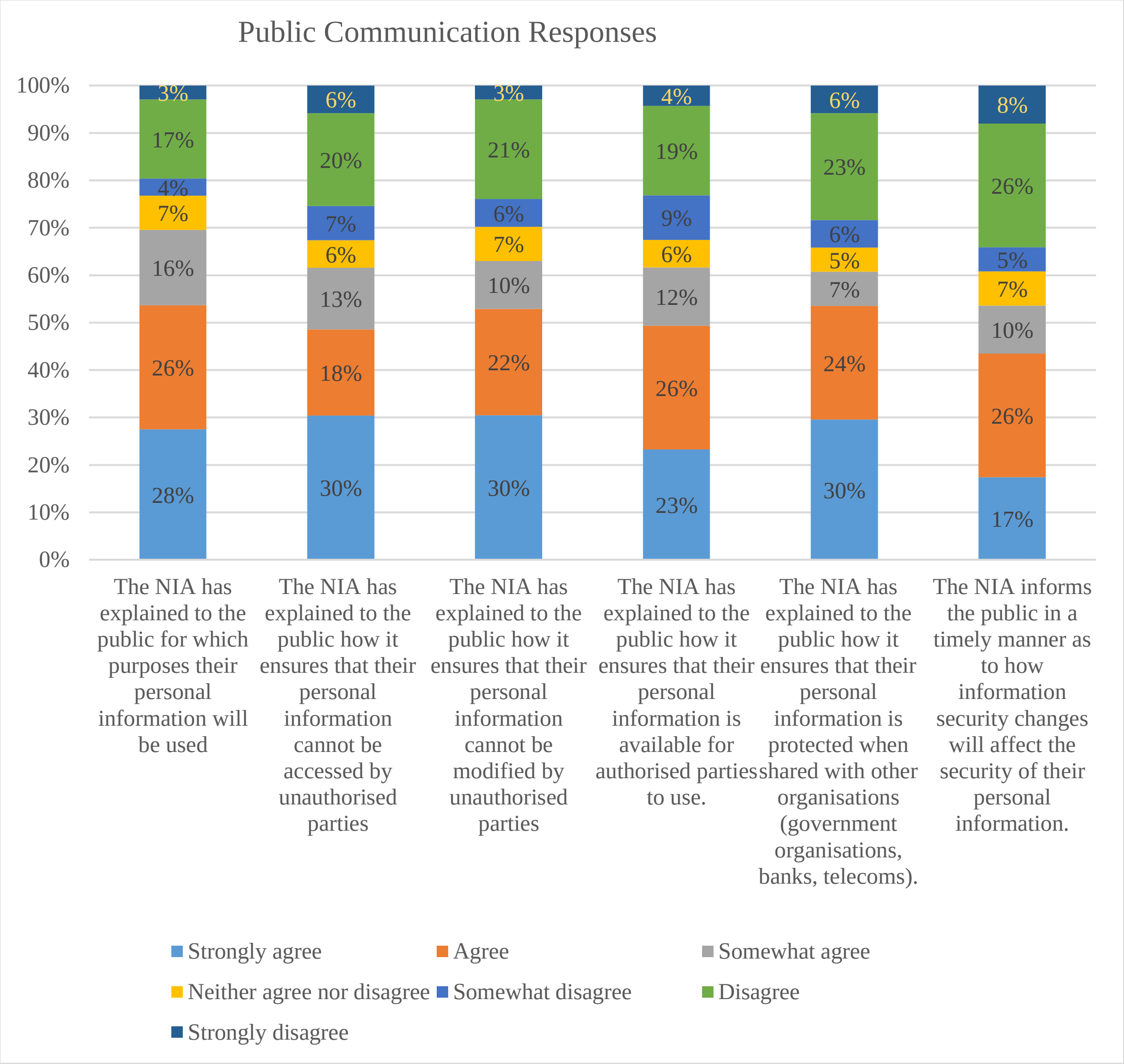


Figure 30: NIA Public Communication Distribution

To understand the differences in public communication expectations based on gender, we analysed the responses of male and female participants separately. This analysis helps to identify any gender-specific trends or biases in public expectations (See Appendix 9.10, Figure 42). We noted that cumulatively, the females were more positive about the use and purposes of personal information than the males (80% vs 65%). The females were also slightly more assertive with their confidence levels (28% vs 27%).

On personal information accessed by unauthorised persons, both males and females were cumulatively positive, with the females being slightly ahead (65% vs 61%). However, the males were comparatively more confident in their responses (30% vs 31%).

On the NIA, having explained to the public how it ensures that unauthorised parties cannot modify their personal information, 67% of the females and 62% of the males were cumulatively positive with their responses. In comparison, 30% of the females and 31% of the males agreed with the question. This means the females were slightly more confident and optimistic in their responses.

On “NIA has explained to the public how it ensures that their personal information is available for authorised parties to use”, the males were both more confident and more positive in their responses than the females (cumulatively 63% for males vs 59% for females and 19% vs 25% for strongly agree).

Again, on “The NIA has explained to the public how it ensures that their personal information is protected when shared with other organisations (government organisations, banks, telecoms)”, 28% of the females compared to 31% of the males strongly agreed. This means that the males were more confident in their responses. Cumulatively, however, the females were more positive in their reactions than their male counterparts were (63% of females vs 61% of males).

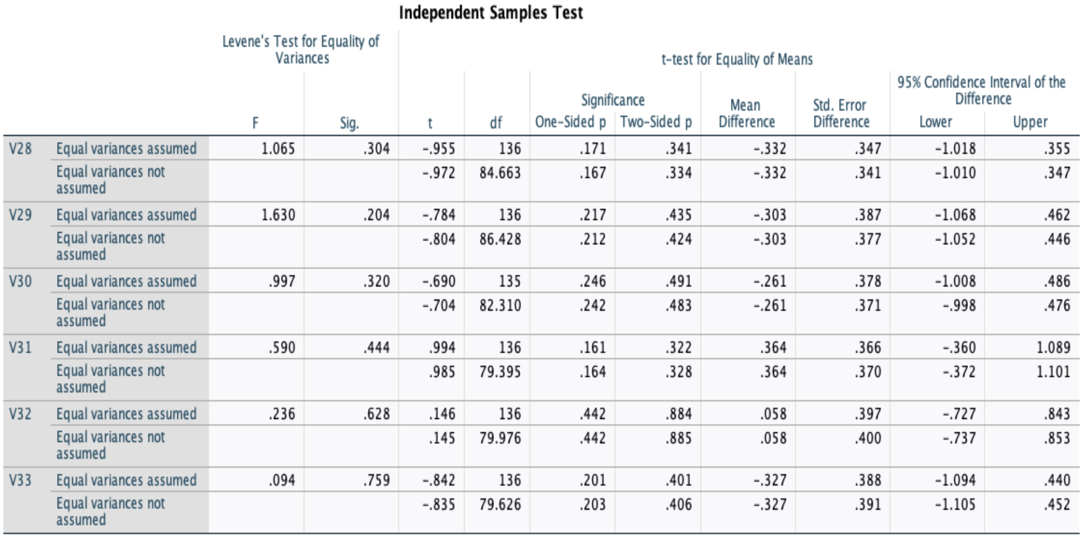
Finally, on the “The NIA informs the public in a timely manner as to how information security changes will affect the security of their personal information”, 23% of females and 15% of males strongly agreed. This means that the females were more confident than their male counterparts. Cumulatively, 58% of the females were positive in their responses, while 52% of the males were positive in their responses. This means that the females were more positive and confident in their responses than their male counterparts.

We calculated and used the Mean and the Standard Deviation to analyse the central tendency of the data. Standard Deviation was used to know the range of the data or measure of dispersion for the data in line with Stevens’ measurement framework where Likert scale-type items are summed or averaged and presented horizontally (Uebersax, 2006). The details are as presented below:

Question	Gender	Mean	Std. Deviation
The NIA has explained to the public for which purposes their personal information will be used.	Female	2.72	1.830
	Male	3.05	1.915
The NIA has explained to the public how it ensures that their personal information cannot be accessed by unauthorised parties.	Female	3.02	2.006
	Male	3.33	2.146
The NIA has explained to the public how it ensures that their personal information cannot be modified by unauthorised parties	Female	2.93	1.968
	Male	3.19	2.070
The NIA has explained to the public how it ensures that their personal information is available for authorised parties to use.	Female	3.51	2.028
	Male	3.15	1.978
The NIA has explained to the public how it ensures that their personal information is protected when shared with other organisations (government organisations, banks, telecoms).	Female	3.28	2.186
	Male	3.22	2.150
The NIA informs the public in a timely manner as to how information security changes will affect the security of their personal information.	Female	3.44	2.141
	Male	3.77	2.096

Table 18: Mean and Standard Deviation on NIA Public Communication

From Table 17, the results reveal differences in the mean responses of female and male respondents regarding the communication of their personal information handling. For instance, females agreed more strongly than males on the importance of the NIA explaining the purposes for which their personal information will be used (mean of 2.72 for females vs. 3.05 for males). However, the t-test results (Figure 31) show no statistically significant differences between male and female responses, indicating that gender does not significantly influence public communication expectations as presented below:



Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means							
						Significance				95% Confidence Interval of the Difference	
		F	Sig.	t	df	One-Sided p	Two-Sided p	Mean Difference	Std. Error Difference	Lower	Upper
V28	Equal variances assumed	1.065	.304	-.955	136	.171	.341	-.332	.347	-1.018	.355
	Equal variances not assumed			-.972	84.663	.167	.334	-.332	.341	-1.010	.347
V29	Equal variances assumed	1.630	.204	-.784	136	.217	.435	-.303	.387	-1.068	.462
	Equal variances not assumed			-.804	86.428	.212	.424	-.303	.377	-1.052	.446
V30	Equal variances assumed	.997	.320	-.690	135	.246	.491	-.261	.378	-1.008	.486
	Equal variances not assumed			-.704	82.310	.242	.483	-.261	.371	-.998	.476
V31	Equal variances assumed	.590	.444	.994	136	.161	.322	.364	.366	-.360	1.089
	Equal variances not assumed			.985	79.395	.164	.328	.364	.370	-.372	1.101
V32	Equal variances assumed	.236	.628	.146	136	.442	.884	.058	.397	-.727	.843
	Equal variances not assumed			.145	79.976	.442	.885	.058	.400	-.737	.853
V33	Equal variances assumed	.094	.759	-.842	136	.201	.401	-.327	.388	-1.094	.440
	Equal variances not assumed			-.835	79.626	.203	.406	-.327	.391	-1.105	.452

Figure 31: T-Test Results on NIA Public Communication

The t-test results confirm that none of the differences in mean responses between male and female participants are statistically significant.

7.4.3.3 NIA Public Trust

NIA Competence

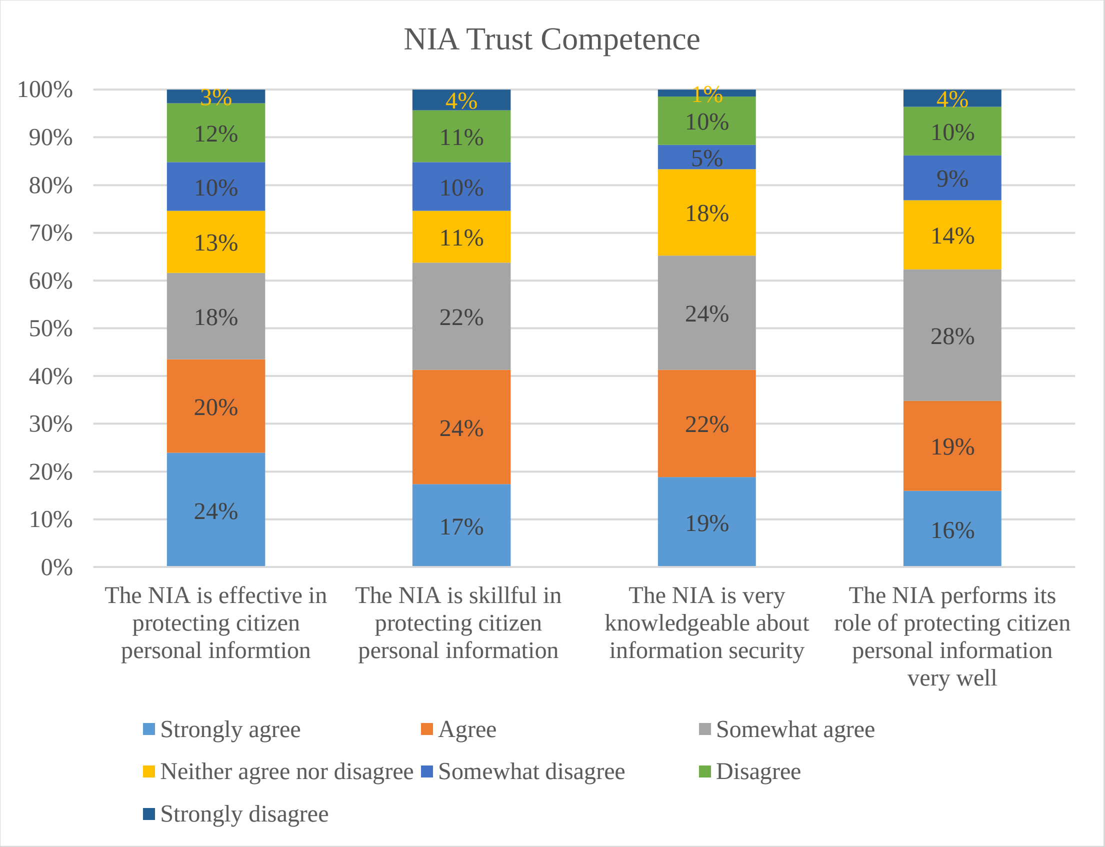


Figure 32: NIA Trust Competence Distribution

From Figure 32, the majority of respondents generally believe that the NIA is effective in protecting their personal information (62%, 85 respondents), skilful in protecting their personal information (63%, 87 respondents), knowledgeable about information security (65%, 89 respondents), and performs their role of safeguarding citizen personal information very well (63%, 87 respondents). However, a substantial minority disagrees, with 25% (33 respondents) for protecting their personal information, 25% (33 respondents) for being skilful in protecting their personal information, 16% (22 respondents) for performing their role of protecting citizens' personal information very well, and 23% (32 respondents) for performing their role of safeguarding citizen personal information very well. Additionally, some respondents remained neutral: 13% (18 respondents) for protecting their personal information, 11% (15 respondents) for being skilful in protecting their personal information, 18% (25 respondents) for performing their role of protecting citizens' personal information very well, and 14% (20 respondents) for fulfilling their role of safeguarding citizens' personal information very well.

Gender Distribution on NIA Trust Competence

To understand the differences in trust competence based on gender, we analysed the responses of male and female participants separately. This analysis helps to identify any gender-specific trends or biases in public trust (See Appendix 9.10, Figure 43). The NIA trust, cumulatively shows that the female members of the public were more positive about the effectiveness of the NIA in protecting citizens' personal information than their male counterparts (63% vs 61%). On the NIA being skilful in protecting citizens' personal information, the females were more optimistic than their male counterparts (72% vs 60%). On the NIA being knowledgeable about information security, the data shows that the females were more optimistic than their male counterparts (67% vs 64%). In contrast, on the NIA performing its role of protecting citizens' personal information very well, the males were more positive than the females (66% vs 56%).

Mean and Standard Deviation on NIA Trust Competence

Question	Gender	Mean	Std. Deviation
The NIA is effective in protecting personal information	Female	2.72	1.830

	Male	3.05	1.915
The NIA is skillful in protecting personal information	Female	3.02	2.006
	Male	3.33	2.146
The NIA is knowledgeable about information security	Female	2.93	1.968
	Male	3.19	2.070
The NIA performs its role of safeguarding personal information very well	Female	3.51	2.028
	Male	3.15	1.978

Table 19: Mean and Standard Deviation on NIA Trust Competence

From Table 18, the results reveal differences in the mean responses of female and male respondents regarding trust competence. For instance, females agreed more strongly than males on the effectiveness of the NIA in protecting personal information (mean of 2.72 for females vs. 3.05 for males). However, the t-test results show no statistically significant differences between male and female responses, indicating that gender does not significantly influence trust competence expectations.

The t-test results confirm that none of the differences in mean responses between male and female participants are statistically significant.

NIA Benevolence

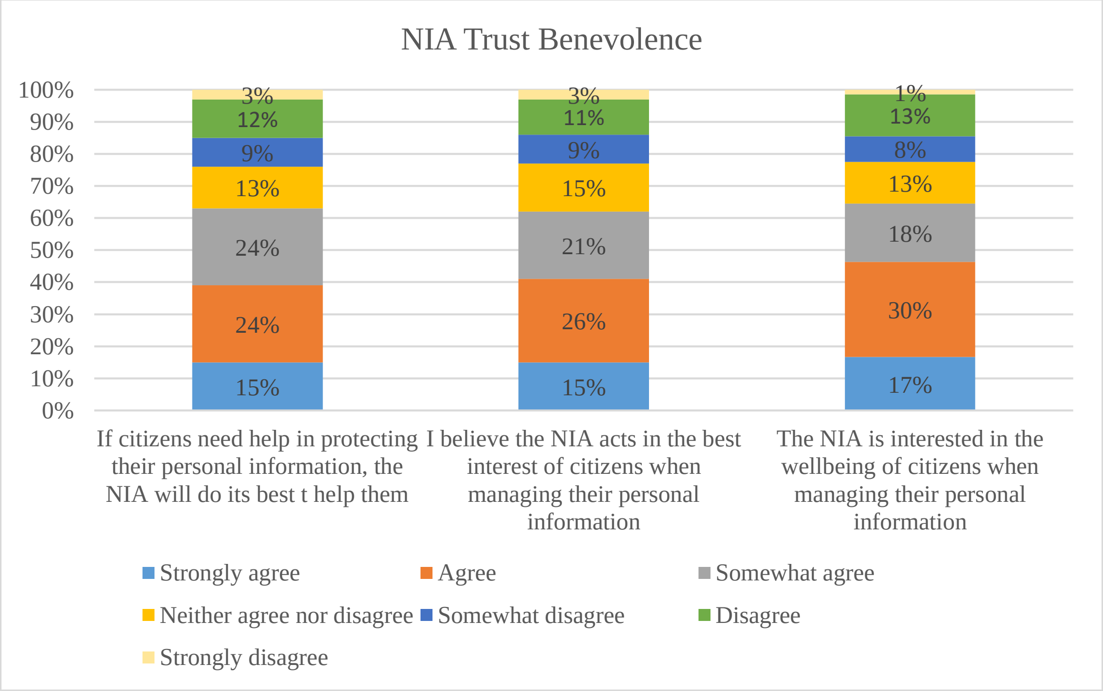


Figure 33: NIA Trust Benevolence Distribution

The responses on NIA Trust benevolence show that 63% (87 respondents) cumulatively agree that the NIA will do its best to help citizens if they need it, 62% (85 respondents) believe that the NIA acts in the best interest of the citizens when managing their personal information, and 65% (89 respondents) agree that the NIA is interested in the well-being of citizens when collecting their data. However, a substantial minority disagree cumulatively. On this, 24% (33 respondents) were on the NIA doing its best to help citizens, 23% (32 respondents) were on the NIA acting in the best interest of citizens, and 22% (30 respondents) were on the NIA being interested in the well-being of citizens. Additionally, some respondents remained neutral: 13% (18 respondents) on the NIA doing its best to help citizens, 15% (21 respondents) on the NIA acting in the best interest of citizens, and 13% (18 respondents) on the NIA being interested in the well-being of citizens.

Gender Distribution on NIA Trust Benevolence

To understand the differences in trust benevolence based on gender, we analysed the responses of male and female participants separately. This analysis helps to identify any gender-specific trends or biases in public trust benevolence (See Appendix 9.10, Figure 44). gender distribution of NIA Trust benevolence, the male and female members of the public were in equal agreement on the NIA doing its best to help citizens if they need it (63% vrs 63%). On the belief that the NIA acts in the best interest of the citizens when managing their personal information, the males were more positive than the females (64% vrs 58%). On the NIA being interested in the well-being of citizens when managing their personal information, the females were more optimistic (65vrs 64).

The females were more neutral on both “I believe the NIA acts in the best interest of citizens when managing their personal information” and “The NIA is interested in the wellbeing of citizens when managing their personal information”. However, the males were more neutral: "If citizens need help in protecting their personal information, the NIA will do its best to help them”.

On the disagreement, while 26% of females cumulatively disagree, 23% of males disagree on “If citizens need help in protecting their personal information, the NIA will do its best to help them”. 23% of females cumulatively disagree on “I believe the NIA acts in the best interest of citizens when managing their personal information”, while 22% of males believe the same to be the case. On the NIA's interest in the well-being of citizens when managing their personal information, 21% of females cumulatively disagreed, while 23% of males disagreed.

Mean and Standard Deviation on NIA Trust Competence

Question	**Gender**	**Mean**	**Std. Deviation**
The NIA will do its best to help citizens if they need it	Female	3.44	2.141
	Male	3.77	2.096
The NIA acts in the best interest of citizens when managing personal information	Female	3.28	2.186
	Male	3.22	2.150
The NIA is interested in the well-being of citizens when collecting data	Female	3.51	2.028
	Male	3.15	1.978

Table 20: Means and Standard Deviation on NIA Trust Benevolence

Table 19 reveals differences in the mean responses of female and male respondents regarding trust benevolence. For instance, females agreed more strongly than males on the NIA doing its best to help citizens (mean of 3.44 for females vs. 3.77 for males). However, the t-test results show no statistically significant differences between male and female responses, indicating that gender does not significantly influence trust benevolence expectations.

The t-test results confirm that none of the differences in mean responses between male and female participants are statistically significant.

NIA Integrity

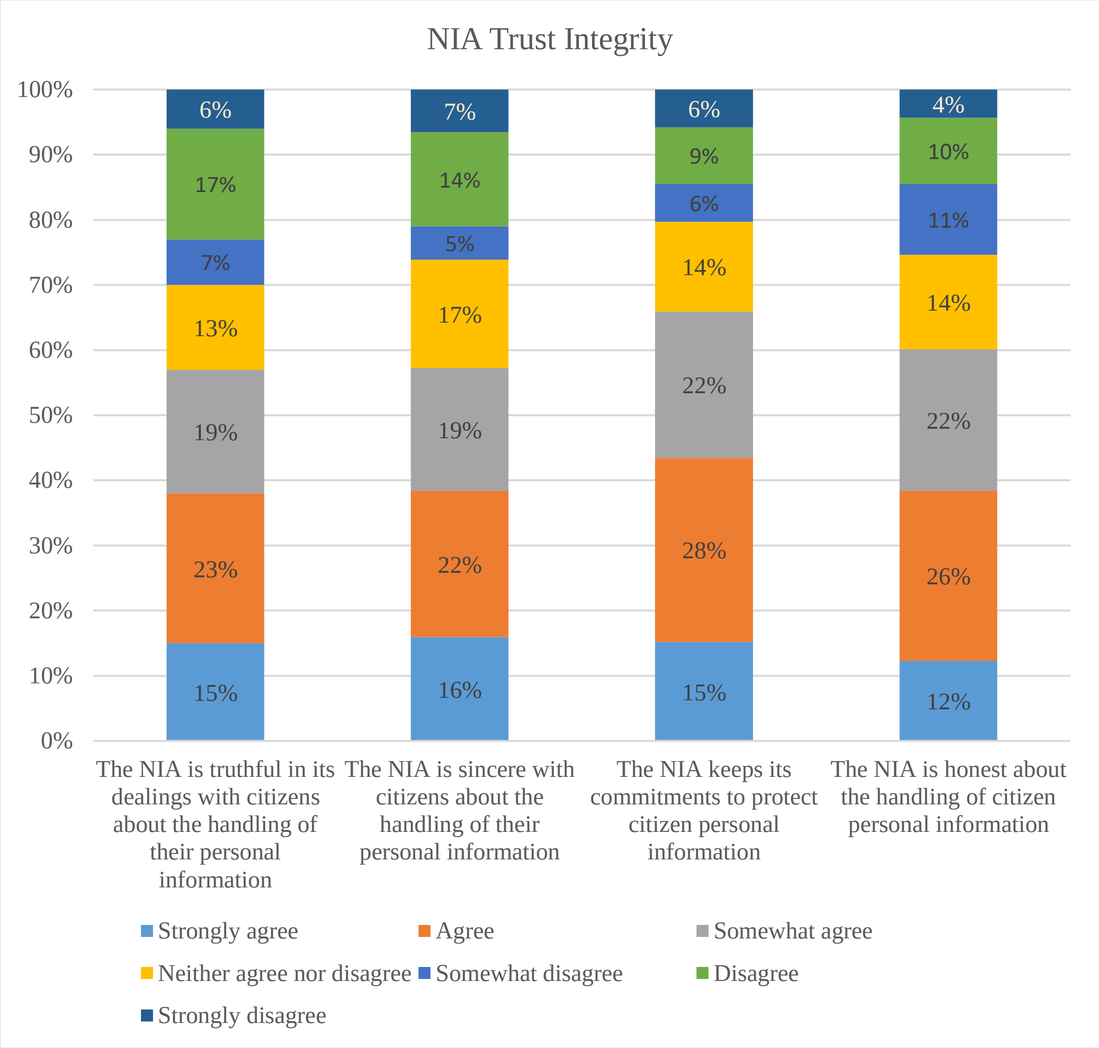


Figure 34: NIA Trust Integrity Distribution

On NIA Trust Integrity, 57% (78 respondents) of the public members cumulatively agree that the NIA is truthful in dealing with staff handling of personal information, 57% (78 respondents) agree with the sincerity of the NIA with citizens about handling their personal data, 65% (89 respondents) agree that the NIA keeps its commitment to protecting citizens' personal information, and 60% (82 respondents) agree with the honesty of the NIA about handling citizens' personal information. However, a substantial minority disagrees: 30% (41 respondents) on the NIA being truthful, 26% (36 respondents) on the sincerity of the NIA, 21% (29 respondents) on the NIA keeping its commitments, and 25% (34 respondents) on the honesty of the NIA. Additionally, some respondents remained neutral: 13% (18 respondents) on truthfulness, 17% (23 respondents) on sincerity, 14% (19 respondents) on keeping commitments, and 14% (20 respondents) on honesty.

Gender Distribution on NIA Trust Integrity

To understand the differences in trust integrity based on gender, we analysed the responses of male and female participants separately. The gender distribution of public responses on NIA Trust Integrity (See Appendix 9.10, Figure 45) reveals that the males were more positive than the females on both NIA being truthful in handling personal information (59% vs 52%) and being sincere with citizens about handling their data (60% vs 51%). On the belief that the NIA acts in the best interest of the citizens when managing their personal information, the males were more positive than the females (64% vs 58%). Further, the males were more optimistic about the NIA keeping its commitments (69% vs 54%). On the honesty of the NIA about handling the citizens' personal information, the males were more optimistic than their female counterparts (52 vs 64%). This means that the males were more positive about the NIA Trust's integrity.

However, some males and females either disagreed or remained neutral.

The females were more neutral on all questions except the truthfulness in dealing with citizens' personal information, which was 12% versus 14%. The ones favouring females were 19% vs 16% on sincerity, 21% vs 11% on keeping commitments and 23% vs 11% on honesty.

On the disagreement, while 36% of females cumulatively disagreed, 27% of males disagreed on the truthfulness. 30% of the females were in dispute, while 24% of the males disagreed about the sincerity of the NIA in handling citizen data. On the keeping of commitments, while 21% of the females disagreed, 19% of the males disagreed. On the honesty of the NIA in handling citizens' personal information, 25% of the females disagreed, and 24% of the males disagreed.

Table: Mean and Standard Deviation on NIA Trust Integrity

Question	**Gender**	**Mean**	**Std. Deviation**
The NIA is truthful in handling personal information	Female	3.44	2.141
	Male	3.77	2.096
The NIA is sincere with citizens about handling their data	Female	3.28	2.186
	Male	3.22	2.150

The NIA keeps its commitments to protect personal information	Female	3.51	2.028
	Male	3.15	1.978
The NIA is honest about handling citizens' personal information	Female	3.44	2.141
	Male	3.77	2.096

Table 21: Mean and Standard Deviation on NIA Trust Integrity

From the table, the results reveal differences in the mean responses of female and male respondents regarding trust integrity. For instance, females agreed more strongly than males on the NIA being truthful in handling personal information (mean of 3.44 for females vs. 3.77 for males). However, the t-test results show no statistically significant differences between male and female responses, indicating that gender does not significantly influence trust integrity expectations.

The t-test results confirm that none of the differences in mean responses between male and female participants are statistically significant.

7.4.3.4 NIA Staff Trust

Staff Trust Competence

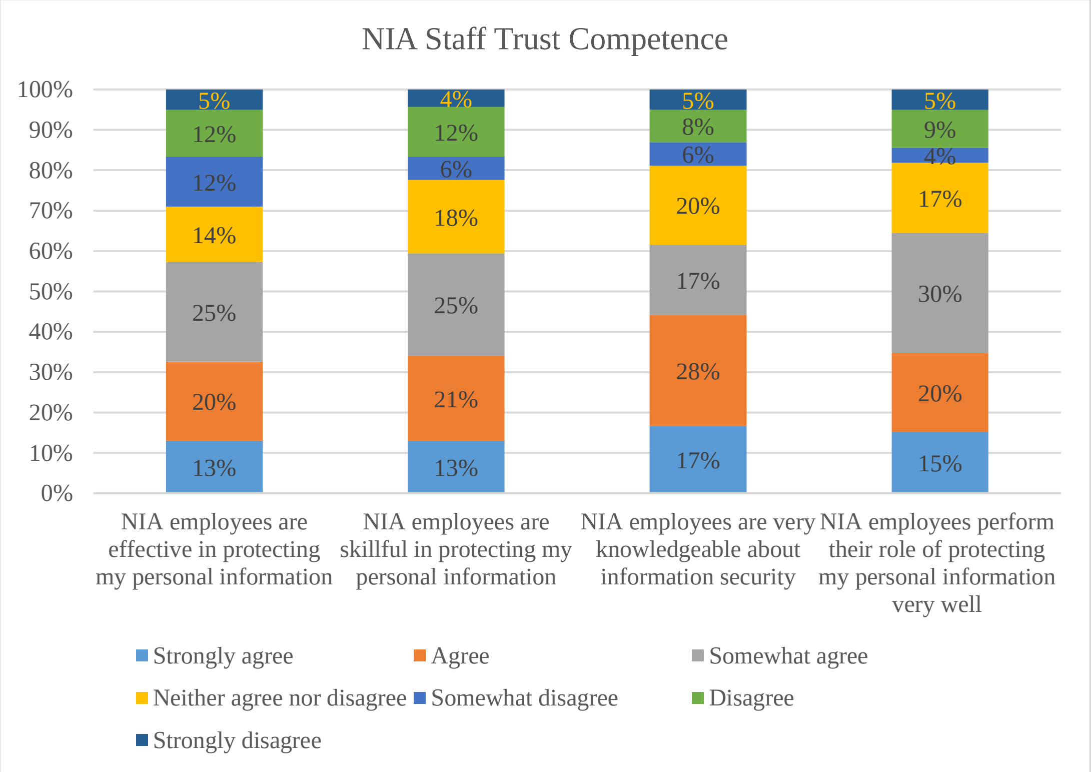


Figure 35: NIA Staff Trust Distribution

From Figure 35, the majority of respondents generally believe that NIA employees are effective in protecting personal information (58%, 79 respondents), skilful in protecting personal information (59%, 81 respondents), knowledgeable about information security (62%, 85 respondents), and perform their role of protecting personal information very well (65%, 89 respondents). However, a substantial minority disagrees, with 29% (40 respondents) for effectiveness, 22% (30 respondents) for skilfulness, 19% (26 respondents) for knowledge, and 18% (25 respondents) for performance in protecting personal information. Additionally, some respondents remained neutral: 14% (19 respondents) for effectiveness, 18% (25 respondents) for skilfulness, 20% (27 respondents) for knowledge, and 17% (23 respondents) for performance.

Gender Distribution on NIA Staff Trust Competence

To understand the differences in trust competence based on gender, we analysed the responses of male and female participants separately. This analysis helps to identify any gender-specific trends or biases in the public trust competence of the NIA Staff Trust (See Appendix 9.10, Figure 46). The gender distribution of responses for NIA Staff Trust competence reveals that the females were cumulatively more optimistic than their male counterparts (59% of females versus 57% of males) on NIA employee's effectiveness in protecting personal information. Again, on NIA employees' skills in safeguarding personal information, the females were cumulatively more optimistic than their male counterparts (63% females vs 58% males). Regarding NIA employees' information security knowledge, the females were more positive in their responses than the males (63% females vs 61% males). In comparison, in the case of NIA employees performing their role in protecting personal information very well, the males were more positive than the females (65% males versus 63% females). This means that, overall, the females were more positive in their responses on all NIA Staff Trust competence questions except on NIA employees performing their role in protecting personal information very well.

However, some males and females in each category either disagreed or remained neutral. The males were more neutral on all questions than the females on NIA Staff Trust competence.

On the disagreement, while 30% of females cumulatively disagreed, 29% of males disagreed on NIA employees' effectiveness in protecting personal information. 21% of the females were in disagreement, while 23% of the males were in dispute on NIA employees' skills in safeguarding personal information. Regarding NIA employees' knowledge about information security, 19% of the females and 18% of the males disagreed. On NIA employees performing their role in protecting personal information very well, 21% of the females disagreed, and 17% of the males disagreed.

Mean and Standard Deviation on NIA Staff Trust Competence

Question	**Gender**	**Mean**	**Std. Deviation**
NIA employees are effective in protecting personal information	Female	2.72	1.830
	Male	3.05	1.915
NIA employees are skillful in protecting personal information	Female	3.02	2.006
	Male	3.33	2.146
NIA employees are knowledgeable about information security	Female	2.93	1.968
	Male	3.19	2.070
NIA employees perform their role of protecting personal information very well	Female	3.51	2.028
	Male	3.15	1.978

Table 22: Mean and Standard Deviation on NIA Staff Trust Benevolence

From the table, the results reveal differences in the mean responses of female and male respondents regarding trust competence. For instance, females agreed more strongly than males on the effectiveness of NIA employees in protecting personal information (mean of 2.72 for females vs. 3.05 for males). However, the t-test results show no statistically significant differences between male and female responses, indicating that gender does not significantly influence trust competence expectations.

The t-test results confirm that none of the differences in mean responses between male and female participants are statistically significant.

NIA Staff Benevolence

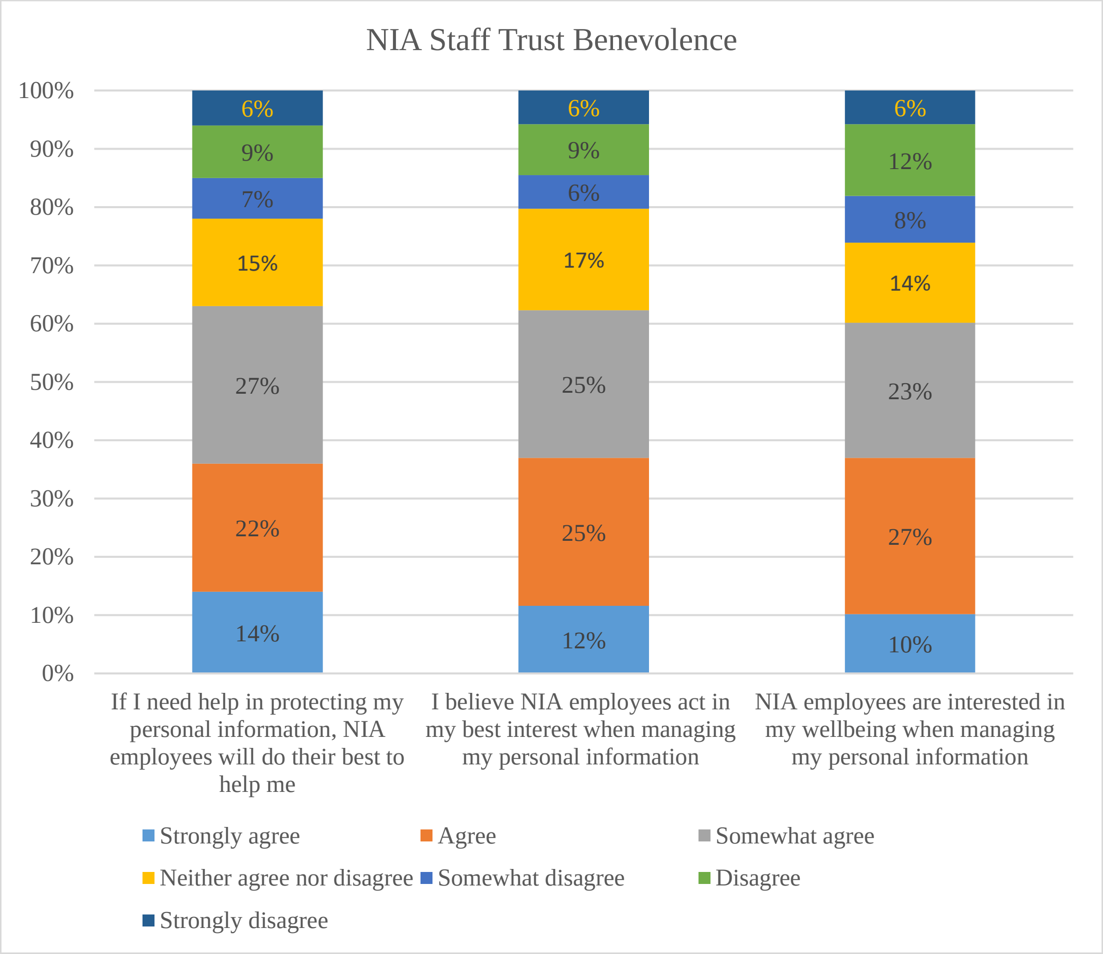


Figure 36: NIA Staff Trust Benevolence Distribution

From Figure 36, the majority of respondents generally believe that NIA staff are benevolent in their actions. Specifically, 63% (86 respondents) agree that if citizens need help protecting their personal information, NIA staff will do their best to help them. Similarly, 62% (85 respondents) believe that NIA staff act in the best interest of citizens when managing their personal information, and 60% (82 respondents) agree that NIA staff are interested in the well-being of citizens when managing their data. However, a substantial minority disagrees, with 22% (30 respondents) for helping protect personal information, 21% (29 respondents) for acting in the best interest of citizens, and 26% (36 respondents) for being interested in the well-being of citizens. Additionally, some respondents remained neutral: 15% (21 respondents) for helping protect personal information, 17% (23 respondents) for acting in the best interest of citizens, and 14% (19 respondents) for being interested in the well-being of citizens.

Gender Distribution on NIA Staff Trust Benevolence

To understand the differences in trust benevolence based on gender, we analysed the responses of male and female participants separately. This analysis helps to identify any gender-specific trends or biases in public trust on NIA Staff Trust Benevolence (See Appendix 9.10, Figure 47). The gender distribution of responses shows that, the females were cumulatively more optimistic than their male counterparts (73% of females vs 59% of males) on the citizen's help by NIA staff in protecting their personal information. However, the males were cumulatively more optimistic than their female counterparts (64% males vs 58% females) on the NIA staff acting in the best interest of respondents when managing their personal information. On NIA staff being interested in respondents' well-being when managing their personal information, the females and the males were equally positive (60% females versus 60% males) in their responses. This means that on NIA Staff's benevolence, the general observation highlights that while the females were more optimistic about NIA staff doing their best to help respondents protect their personal information, the males were also more positive about NIA staff acting in citizens' best interest when managing their personal information. However, males and females were equal in response to NIA staff being interested in citizens' well-being when managing their personal information.

On the gender response distribution for neutral and disagreement, the males were more neutral on the NIA staff doing their best to help the members of the public when they need help (9% females vs 18% males). On the NIA staff acting in the best interest of respondents when managing their personal information, the females were more neutral than the males (21% females vs 16% males). On NIA employees interested in the wellbeing of the members of the public when managing personal information, the females were more neutral than the males (19% females vs 12% males).

On the disagreement, 19% of females cumulatively disagreed, and 23% of males disagreed on the NIA staff doing their best to help the members of the public when they need help with personal information. In addition, 21% of the females were in disagreement, while 19% of the males disagreed when it came to believing that the NIA staff acted in the best interest of respondents when managing their personal information. On NIA employees interested in the well-being of the members of the public when managing personal information, 22% of the females disagreed, and 28% of the males disagreed.

Mean and Standard Deviation on NIA Staff Trust Benevolence

Question	**Gender**	**Mean**	**Std. Deviation**
NIA staff will do their best to help citizens protect personal information	Female	2.72	1.830
	Male	3.05	1.915
NIA staff act in the best interest of citizens when managing personal information	Female	3.02	2.006
	Male	3.33	2.146
NIA staff are interested in the well-being of citizens when managing personal information	Female	2.93	1.968
	Male	3.19	2.070

Table 23: Mean and Standard Deviation NIA Staff Trust Benevolence

Table 22 reveals differences in the mean responses of female and male respondents regarding trust benevolence. For instance, females agreed more strongly than males on NIA staff doing their best to help citizens protect personal information (mean of 2.72 for females vs. 3.05 for males). However, the t-test results show no statistically significant differences between male and female responses, indicating that gender does not significantly influence trust benevolence expectations.

The t-test results confirm that none of the differences in mean responses between male and female participants are statistically significant.

NIA Staff Integrity

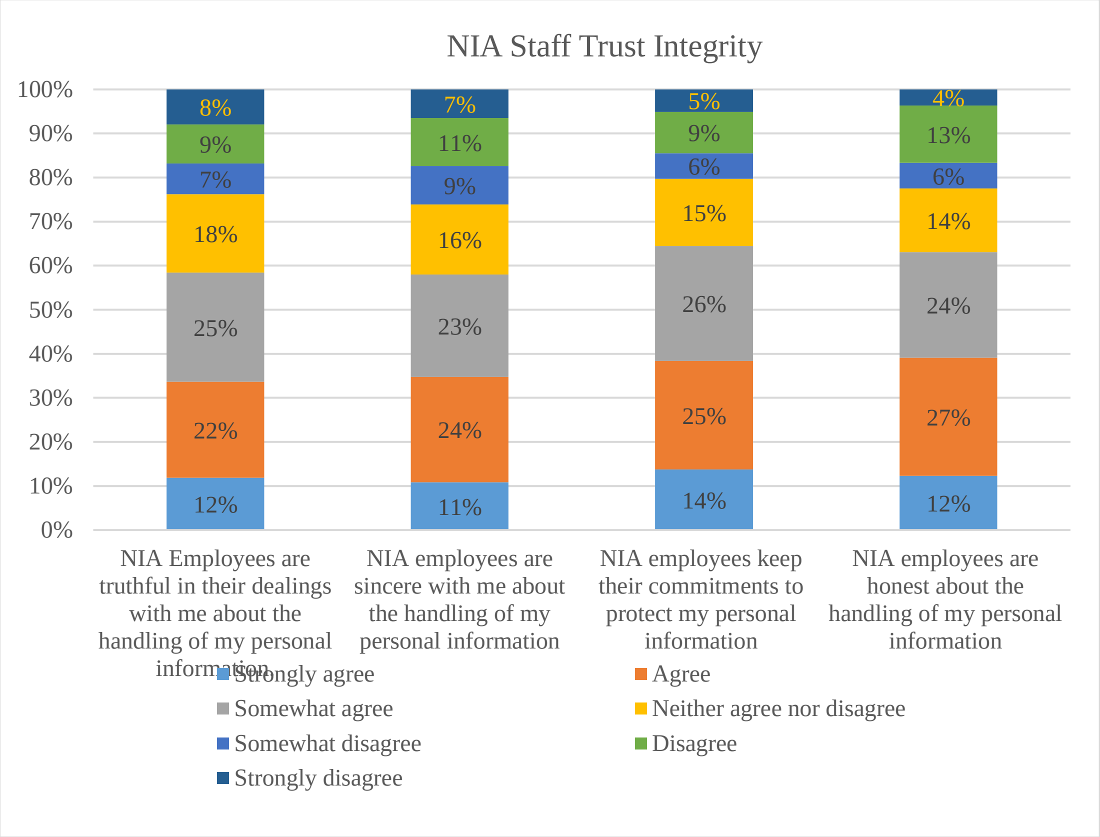


Figure 37: NIA Staff Trust Integrity Distribution

From Figure 37, the majority of respondents generally believe that NIA employees are trustworthy in their actions. Specifically on NIA Staff Trust Integrity, the members of the public responses indicate that 59% (81 respondents) cumulatively agreed that the NIA employees are truthful in dealing with them when handling their personal information. Cumulatively, 58% (80 respondents) of the public members decided that the NIA employees were sincere when handling their data. In addition, 65% (89 respondents) of the respondents agreed that the NIA employees keep their commitments to protect their personal information. 63% (86 respondents) of the respondents also shared their cumulative agreement that the NIA employees are honest about the handling of personal information.

Regarding disagreements, 23% (32 respondents) cumulatively disagreed that the NIA employees are truthful in dealing with them when handling their personal information. 27% (38 respondents) disagreed that the NIA employees are sincere when handling their data. 20% (27 respondents) also cumulatively disagreed that the NIA employees kept to their commitments to protect their personal information, and 23% (32 respondents) disagreed with the belief that the NIA employees are honest about handling personal data.

Regarding neutrality, 18% (25 respondents), 16% (22 respondents), 15% (21 respondents) and 14% (19 respondents) remained neutral on NIA employees being truthful in their dealings, being sincere, keeping to their commitments and being honest when handling their personal information, respectively.

Overall, most respondents believe that the NIA staff are truthful in their dealings, sincere, keep to their commitments and honest when handling the personal information of the members of the public.

Gender Distribution on NIA Staff Trust Integrity

To understand the differences in trust integrity based on gender, we analysed the responses of male and female participants separately to identify any gender-specific trends or biases in public trust on NIA Staff Trust integrity (Appendix 9.10, Figure 48).

The gender distribution of responses highlights that the females were more positive cumulatively than their male counterparts (61% of females vs 58% for males) on the truthfulness of NIA employees in their dealings with the members of the public in handling their personal information. On NIA employees' sincerity with the members of the public, the females were cumulatively more optimistic than their male counterparts (61% females vs 57% males). The male respondents were more confident than their female counterparts about NIA employees keeping their commitments to protect their personal information (63% females vs 65% males). Regarding the NIA employees' honesty to the public when handling their personal information, the males were cumulatively more positive than the females (61% females vs 67% males).

This means the males and females were divided in responses to NIA Staff integrity. Whereas the females were more positive on two (truthfulness and sincerity), the males were more positive on the other two integrity issues (keeping to their commitments and honesty).

The females were more neutral on the truthfulness of NIA employees to the members of the public than their male counterparts (19% females vs 18% males). However, the males were more neutral on the other three integrity questions about the NIA employees (17% males vs

14% females on sincerity, 16% males vs 14%females on the keeping of commitment and 15% males vs 14% females on honesty).

In terms of gender disagreement, the males were more negative than the females on truthfulness, sincerity and honesty (21% of females vs 23% of males on truthfulness, 27% of males vs 26% of females on sincerity and 23% of males vs 21% of females on honesty). However, the females were more negative about NIA employees keeping their commitment (23% of females vs 18% of males).

Mean and Standard Deviation on NIA Staff Trust Integrity

Question	Gender	Mean	Std. Deviation
NIA employees are truthful in dealing with personal information	Female	2.72	1.830
	Male	3.05	1.915
NIA employees are sincere in handling personal information	Female	3.02	2.006
	Male	3.33	2.146
NIA employees keep their commitments to protect personal information	Female	2.93	1.968
	Male	3.19	2.070
NIA employees are honest about handling personal information	Female	3.51	2.028
	Male	3.15	1.978

Table 24: Mean and Standard Deviation on NIA Staff Trust Integrity

From the table, the results reveal differences in the mean responses of female and male respondents regarding trust integrity. For instance, females agreed more strongly than males on NIA employees being truthful in dealing with personal information (mean of 2.72 for females vs. 3.05 for males). However, the t-test results show no statistically significant differences between male and female responses, indicating that gender does not significantly influence trust integrity expectations.

The t-test results confirm that none of the differences in mean responses between male and female participants are statistically significant.

Comparative Analysis between NIA Trust and NIA Staff Trust

We further carried out an analysis to know the trust levels of the public in the NIA organisation and its staff on each of the trust categories: Competence, Benevolence and Integrity. The details are as follows:

Attribute	**Question**	**NIA Agreement in %**	**NIA Staff Agreement in %**	**NIA Neutral in %**	**NIA Staff Neutral in %**	**NIA Disagreement in %**	**NIA Staff Disagreement in %**
Competence	Performing role of protecting citizens personal information	63%	65%	14%	17%	23%	18%
	knowledgeable about information security	65%	62%	18%	20%	16%	19%
	skilful in protecting citizen personal information	63%	59%	11%	18%	25%	22%
	effectiveness in protecting citizen personal information	62%	58%	13%	14%	25%	29%
Benevolence	interest in citizens' wellbeing	65%	60%	13%	14%	22%	26%
	acting in the best interest of citizens	62%	62%	15%	17%	23%	21%
	helping in protecting personal information	63%	63%	13%	15%	24%	22%

Integrity	honesty in handling citizens' personal information	60%	63%	14%	14%	25%	23%
	Keeping commitments in citizens' personal information	65%	65%	14%	15%	21%	20%
	Sincerity with citizens	57%	58%	17%	16%	26%	27%
	Truthfulness with citizens	57%	59%	13%	18%	30%	23%

Table 25: NIA vs NIA Staff Trust Results

Comparative Analysis of Means and Standard Deviations

Further to the above, we compared the means and standard deviations of the NIA versus its staff Trust levels as detail below:

Trust	Trust theme	Group type	Mean	Standard Deviation
Competence	Effectiveness	NIA	3.15	1.81
		NIA Staff	3.48	1.737
	Skilfulness	NIA	3.23	1.766
		NIA Staff	3.38	1.685
	Knowledgeable	NIA	3.04	1.589
		NIA Staff	3.14	1.703
	Role Performance	NIA	3.28	1.669
		NIA Staff	3.23	1.658
Benevolence	best citizen support	NIA	3.24	1.681
		NIA Staff	3.3	1.702
	acting in citizen best interest	NIA	3.2	1.671
		NIA Staff	3.3	1.663
	interest in citizen wellbeing	NIA	3.11	1.682
		NIA Staff	3.43	1.734
Integrity	Truthfulness	NIA	3.48	1.877
		NIA Staff	3.43	1.738
	Sincerity	NIA	3.42	1.851
		NIA Staff	3.46	1.735
	Keeping Commitments	NIA	3.16	1.723

		NIA Staff	3.23	1.675
	Honesty	NIA	3.61	1.609
		NIA Staff	3.6	1.546

Table 26: NIA vs NIA Staff Trust Mean and Standard Deviation Results

Competence

From Tables 24 and 25 in terms of competence, we can observe that the public is slightly more in agreement on all three out of four attributes where they believe in the NIA as an organisation more than the NIA staff. It is only in performing roles in protecting their information that the public was slightly in agreement with the staff than the organisation.

Another observation is that in terms of neutral responses on competence, the public was more neutral across all four attributes on NIA staff than on NIA as an organisation.

In terms of disagreements, the public was more in disagreement with NIA as an organisation on two attributes (Performing the role of protecting citizens' personal information and skilful in protecting citizens' personal information) and more in disagreement with the other two attributes with the staff (knowledgeable about information security and effectiveness in protecting citizen personal information).

Benevolence

Regarding Benevolence, the table shows that the public was equally in agreement with two attributes (acting in the best interest of citizens and helping to protect personal information). In addition, the public was more in agreement with one attribute (interest in citizens' well-being).

On neutral responses, the public was more neutral on NIA staff than the NIA as an organisation across all three attributes.

For disagreements, the public was more in disagreement on two attributes (acting in the best interest of citizens and helping in protecting personal information) of NIA as an organisation. The public was only more in disagreement about the NIA staff on the "interest in citizens' wellbeing" attribute.

Integrity

From the table, we observe that the public is in more in agreement with NIA Staff on three out of four attributes which included honesty, sincerity and truthfulness in personal information handling. It is only in keeping commitments that the public was in equal agreement with the NIA staff and the NIA as an organisation.

Regarding neutral responses, the public was equally neutral on honesty, more neutral on two attributes of NIA staff (keeping commitments and Truthfulness) and more neutral on one attribute of NIA as an organisation (sincerity).

In terms of disagreements, the public was more in disagreement with NIA as an organisation on all the attributes except sincerity.

Paired Samples Test

Paired Samples Test									
	PairedDifferences					**t**	**df**	**Significance**	
	Mean	**Std. Deviation**	**Std. Error Mean**	**95% Confidence Interval of the Difference**				**One-Sided p**	**Two-Sided p**
				Lower	Upper				
Competence									
Effectiveness	-.277	1.489	.127	-.529	-.026	-2.181	136	.015	.031
Skilfulness	.000	1.419	.121	-.239	.239	.000	137	.500	1.000
Knowledgeable	-.051	1.303	.111	-.270	.169	-.457	137	.324	.648
Role Performance	.094	1.226	.104	-.112	.301	.903	137	.184	.368
Benevolence									

best citizen support	.000	1.226	.104	-.206	.206	.000	137	.500	1.000
acting in citizen best interest	-.036	1.298	.110	-.255	.182	-.328	137	.372	.743
interest in citizen wellbeing	-.261	1.222	.104	-.467	-.055	-2.508	137	.007	.013
Integrity									
Truthfulness	.065	1.160	.099	-.130	.261	.660	137	.255	.510
Sincerity	-.043	1.207	.103	-.247	.160	-.423	137	.336	.673
Keeping Commitments	-.080	.989	.084	-.246	.087	-.946	137	.173	.346
Honesty	.043	.818	.070	-.094	.181	.624	137	.267	.534

Table 27: NIA vs NIA Staff Trust t-test Results

Further to the above, the t-test results from the table above (table 26) show statistical significance between the trust variables across all pairs. This means the public has strong trust levels in the NIA and the Staff. In more specific details, the following are the observations:

- Regarding Competence Effectiveness, the statistical significance result (Two-Sided p) was 0.031 with a mean of -2.77. The negative mean difference indicates that the public perceives NIA staff as slightly less effective in protecting personal information compared to the NIA organisation. The p-value of 0.031 suggests this difference is statistically significant at the 0.05 level.

- Regarding competence skilfulness, the recorded statistical significance result (Two-Sided p) was 1.0 with a mean of 0.00. This means that there is no difference in the perceived skilfulness between NIA staff and the NIA organisation and the p-value of 1.000 confirms that the difference is not statistically significant.
- Regarding Competence Knowledgeable, the recorded statistical significance result (Two-Sided p) was 0.648 with a mean of -0.051. The small negative mean difference indicates a slight perception that NIA staff are less knowledgeable about information security compared to the NIA organisation. However, the p-value of 0.648 indicates that this difference is not statistically significant.
- Regarding Competence Role Performance, the recorded statistical significance result (Two-Sided p) was 0.368 with a mean of 0.094. Though the positive mean difference suggests that the public perceives NIA staff as slightly better in performing their role of protecting personal information, however, the p-value of 0.368 indicates that this difference is not statistically significant.
- Regarding Benevolence (Best Citizen Support), the recorded statistical significance result (Two-Sided p) was 1.000 with a mean of 0.000. This means there is no difference in the perceived support provided by NIA staff and the NIA organisation. The p-value of 1.000 confirms that this difference is not statistically significant
- Regarding Benevolence (Acting in the Citizen Best Interest), the recorded statistical significance result (Two-Sided p) was 0.743 with a mean of -0.036. The recorded small negative mean difference indicates a little perception that NIA staff act less in the best interest of citizens compared to the NIA organisation. However, the p-value of 0.743 indicates that this difference is not statistically significant.
- On Benevolence (Interest in Citizen well-being), the recorded statistical significance result (Two-Sided p) was 0.013 with a mean of -0.261. The negative mean difference indicates that the public perceives NIA staff as less interested in the well-being of citizens compared to the NIA organisation. The p-value of 0.013 suggests this difference is statistically significant at the 0.05 level.
- Regarding Integrity (Truthfulness), the recorded statistical significance result (Two-Sided p) was 0.673 with a mean of 0.043. The small positive mean difference shows that the public perceives NIA staff as slightly more truthful compared to the NIA organisation. However, the p-value of 0.510 indicates that this difference is not statistically significant.

- Regarding Integrity (Sincerity), the recorded statistical significance result (Two-Sided p) was 0.510 with a mean of 0.065. The small negative mean difference indicates a slight perception that NIA staff are less sincere compared to the NIA organisation. However, the p-value of 0.673 indicates that this difference is not statistically significant.
- Regarding Integrity (Keeping Commitments), the recorded statistical significance result (Two-Sided p) was 0.346 with a mean of -0.080. The small negative mean difference indicates a slight perception that NIA staff are less committed compared to the NIA organisation. However, the p-value of 0.346 indicates that this difference is not statistically significant.
- Regarding Integrity (Honesty), the recorded statistical significance result (Two-Sided p) was 0.53446 with a mean of -0.043. The small positive mean difference suggests that the public perceives NIA staff as slightly more honest compared to the NIA organisation. However, the p-value of 0.534 indicates that this difference is not statistically significant.

Overall, the paired samples t-test results indicate that most differences in public trust between the NIA organisation and its staff are not statistically significant. The only significant differences are in the perceived effectiveness of NIA staff in protecting personal information and their interest in the well-being of citizens, with the NIA organisation being favoured in both cases. This means that the public generally trusts both the NIA organisation and its staff, with only minor differences in specific trust attributes.

7.4.3.5 NIA Public involvement – ISP development & evolution

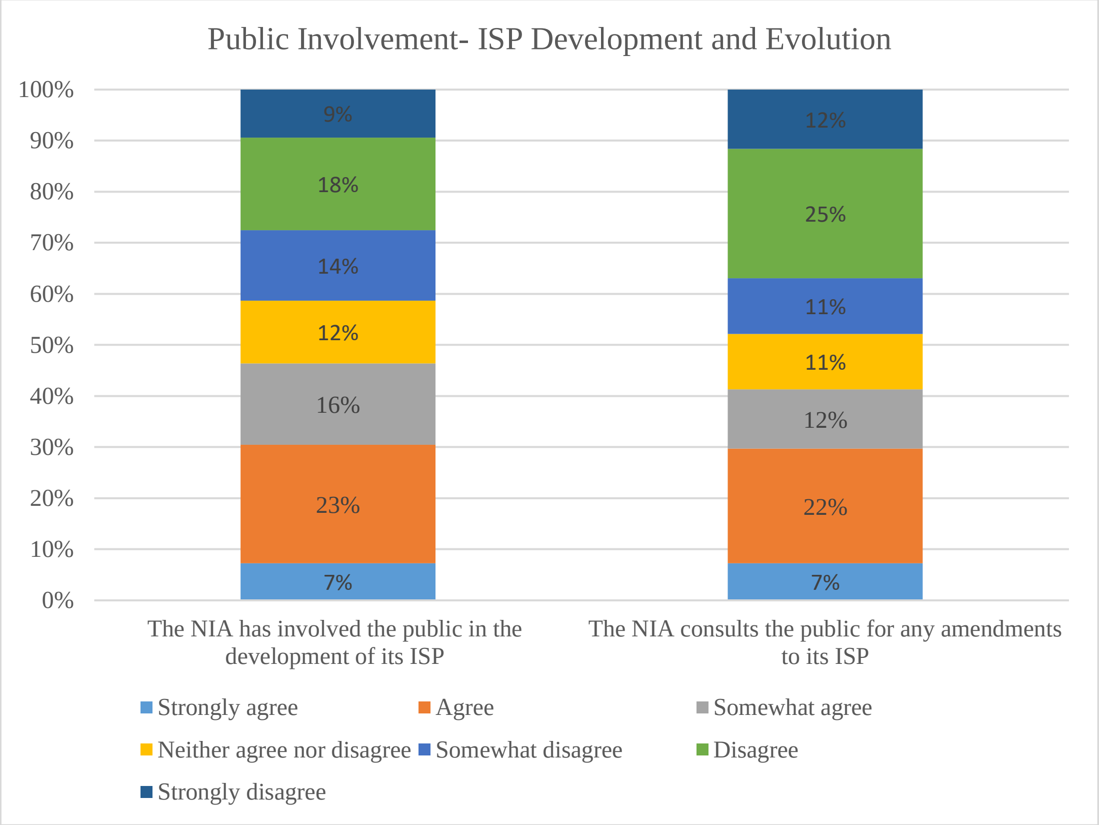


Figure 38: NIA Public involvement – ISP development & evolution Distribution

The responses from the public regarding their involvement in the development and evolution of the NIA ISP indicate a nearly equal division between those who agree and those who disagree. Specifically, 46% of respondents cumulatively agreed that the NIA involves the public in its ISP development, while 41% cumulatively disagreed, and 12% remained neutral. Regarding ISP evolution, 41% agreed that the NIA consults them for ISP amendments, whereas 48% disagreed, and 11% remained neutral. This suggests that while a significant portion of the public feels involved in the development of the ISP, there is a notable perception that they are not adequately consulted during amendments.

Gender Distribution on Public Involvement – ISP Development & Evolution

The gender distribution of public responses ((Appendix 9.10, Figure 49) shows that for ISP development, both males and females equally agree at 46%. However, 42% of females and 41% of males disagreed, while 12% of females and 13% of males remained neutral. This indicates that females were slightly more negative in their responses than males regarding ISP development. For ISP evolution, 44% of females agreed compared to 40% of males.

Disagreement levels were 49% for females and 48% for males, with 7% of females and 13% of males remaining neutral. This suggests that females were more positive and negative than males regarding ISP evolution.

Comparative Analysis of Importance vs. Actual Involvement

We compared the means and standard deviations of the importance of involving the public in ISP development and evolution versus the NIA's actual involvement of the public. The mean for the importance of public involvement in ISP development was 2.17 with a standard deviation of 1.497, while the mean for the NIA's actual involvement was 3.94 with a standard deviation of 1.863. For ISP amendments, the mean for the importance of public involvement was 1.91 with a standard deviation of 1.334, whereas the mean for the NIA's actual involvement was 4.18 with a standard deviation of 1.957. The details are as below in Table 24:

ISP	Trust theme	Group type	Mean	Standard Deviation
Importance	Development	Involvement Views	2.17	1.497
		NIA Actual	3.94	1.863
Participation	Amendments	Involvement Views	1.91	1.334
		NIA Actual	4.18	1.957

Table 28: Mean and Standard Deviation on ISP Development and Evolution (Importance vs actual)

To further confirm the findings, we conducted a paired t-test and the results as presented below in Table 28:

ISP	Trust theme	Group type	t	One-Sided p	Two-Sided p	One-Sided p	Two-Sided p
Importance	Development	Involvement Views	-9.649	0.014	0.028	<0.001	<0.001
		NIA Actual					

Participation	Amendments	Involvement Views	- 12.756	0.003	0.006	<0.001	<0.001
		NIA Actual					

Table 29: T-test Significance on ISP Development and Evolution (Importance vs actual)

The results above indicated a statistically significant difference between the importance of involving the public and the NIA's actual involvement of the public in their ISP development and evolution. For ISP development, the mean difference was significant with a t-value of -9.649 and a p-value of less than 0.001. For ISP amendments, the mean difference was also significant with a t-value of -12.756 and a p-value of less than 0.001. These results suggest that the public perceives a significant gap between the importance of their involvement and the actual involvement by the NIA in both ISP development and amendments. This shows that there is a significant perception among the public that their involvement in the NIA's ISP development and evolution is inadequate compared to its importance. This gap is statistically significant, indicating a need for the NIA to enhance public consultation and involvement in these processes. Despite some differences, the public is almost equally divided between those who agree and those who disagree, with agreement slightly higher for development compared to evolution, where more participants disagree rather than agree. This underscores the importance of addressing public concerns to improve trust and engagement in the ISP processes.

7.5 Discussion

The study findings indicate that although most of the public expects to be involved in the NIA ISP development and revision processes, they are divided on whether they have actually been involved. This aligns with scholarly literature highlighting the importance of stakeholder participation in cybersecurity policy formulation (Von Solms & Von Solms, 2018). The division in responses raises key questions about why some participants may think they have been involved while others do not. It could be that some were involved and others were not due to the process the NIA followed, suggesting a need for broader and more inclusive participation opportunities. Alternatively, it could be that all were involved, but the engagement process was not clear, indicating a need for more transparent public engagement processes.

In addition, the study highlights the need for a framework for assessing the risks and impacts of national electronic identity systems. As discussed in the literature, these frameworks highlight the importance of considering various factors, including social, economic, and political contexts, to provide a holistic assessment of risks (Edu et al., 2023). This comprehensive approach is crucial for understanding the broader impact on stakeholders and ensuring the security and reliability of Electronic identity systems.

Regarding public trust, the results demonstrate that the majority of respondents believe in the NIA's competence, benevolence, and integrity when it comes to managing citizens' personal information. This is congruent with Mayer et al.'s (1995) seminal framework, which posits that trust is built on perceptions of ability, benevolence, and integrity. However, the findings also indicate a significant minority expressing uncertainty or disagreement, highlighting room for improvement in these areas.

Additionally, an investigation into the sources of low public trust in data controllers in Ghana underscores the complexities of data collection, processing, sharing, and utilisation (Collaboration on International ICT Policy for East and Southern Africa [CIPESA], 2022). The study found that mistrust stems from a lack of public education and awareness, as well as personal experiences with data breaches. Effective data governance, which includes robust procedures for data privacy and protection, can foster trust. Data controllers or EIS organisations must therefore comply with legislative and regulatory requirements to build trust with data subjects. Additionally, institutional trust varies significantly across different institutions (OECD, 2024) and highlights the factors influencing trust in public institutions, and they include economic concerns, service satisfaction, and perceptions of fairness and integrity (OECD, 2024).

Regarding political trust in Ghana, the research is in line with the findings that indicate that focusing on both institutional performance and cultural factors plays a significant role in fostering it (Godefroidt, et.al., 2017). The findings suggest that improving government effectiveness and promoting national identity can enhance trust in institutions such as the NIA where the perception of the members of the public about service delivery and organisation are critical due to privacy concerns.

Further to the above, the public's perspectives on NIA's communication about personal data purposes, security, and sharing suggest that while many are satisfied, there is room for improvement. Establishing clear, transparent, and proactive communication channels is vital for building public trust in digital identity systems (Madise & Martens, 2009). Public engagement and consultation are crucial for understanding public needs and concerns, and for building trust in the ID system (World Bank, 2014).

Again, the data on ISP communication vs ISP expectations highlights that the public has higher expectations for both the NIA and its staff relative to communication. However, their responses to the communication questions were, lower compared to their expectations. These relationships highlight the importance of transparency and engagement in building trust by the NIA. This would enhance trust and would reduce the negative perceptions about organisations and their staff. Effective public communication and strong safeguards against undue negative influence are crucial for enhancing trust (OECD, 2024).

The findings also indicate that while the general public has a positive perception of the NIA and its handling of personal information, there are areas for improvement in terms of building public trust. Specifically, the results show that most respondents agreed on the benevolence of NIA staff, but a significant minority did not. This suggests that the NIA should explore strategies to deepen the level of trust in the benevolence of its staff among the public (Mayer & Davis, 1999; Gillespie, 2003; Shockley-Zalabak et al., 2000).

Similarly, the data revealed less confidence among the majority who agreed that NIA employees exhibited integrity, coupled with a sizeable disagreement and neutral position from some respondents. This highlights the need for the NIA to engage better with the public, create awareness, and strategically educate stakeholders to enhance their appreciation of critical trust integrity issues (Cummings & Bromiley, 1996; Robinson, 1996; Clark & Payne, 1997).

The overall findings suggest that while there is a positive perception of the NIA and its handling of personal information, there is room for improvement, particularly in terms of public involvement, communication, and confidence building. This aligns with the literature emphasising the importance of organisations ensuring trust competence, benevolence, and integrity to foster a positive perception among stakeholders (Tyler, 2003; Tzafrir & Dolan, 2004; Spreitzer & Mishra, 1999; McAllister, 1995).

The study’s context-dependent nature, as highlighted by Bachmann (2011), Granovetter (1985), Hardin (2002), McEvily and Tortoriello (2011), and Rousseau et al. (1998), suggests that the trust findings are inherently influenced by specific organisational and societal factors. This underscores the need for the NIA to tailor its trust-building strategies to the unique characteristics and expectations of the Ghanaian public. The context-dependent nature of trust means that the strategies effective in one setting may not be directly applicable in another, emphasising the importance of understanding the local context and adapting strategies accordingly.

Furthermore, the findings emphasise the importance of engaging the public in the development and implementation of information security policies (ISPs) for government-controlled digitised identity systems. Involving the public can help them appreciate the efforts made by the organisation and its staff to protect their data, thereby enhancing trust, data integrity, and security (Warkentin & Johnston, 2010). This public engagement should include training, education, and sensitisation, as well as the development of a clear and comprehensive ISP that addresses trust concerns from the organisational, employee, and public perspectives.

7.6 Concluding Remarks

The findings from this chapter highlight several key conclusions regarding public trust in the National Identification Authority (NIA) and its staff. Firstly, the public has high expectations of data protection, but there is a significant need for improved transparency. Establishing clear, transparent, and proactive communication channels is therefore essential for building public trust in digital identity systems. This aligns with the broader literature on the importance of transparency in fostering trust in public services.

Secondly, the public also has high expectations of engagement, yet the reality falls short of these expectations. The NIA needs to enhance its efforts to meaningfully engage the public in the ISP development and amendment processes. This gap between expectations and reality underscores the importance of stakeholder participation in policy formulation, as emphasised by Von Solms and Von Solms (2018).

Again, Trust in the NIA and its staff is notably higher than trust in public services and public servants in Ghana. However, there remains room for improvement through increased transparency and public engagement. The findings suggest that while the public generally trusts the NIA and its staff, efforts to enhance this trust further are necessary. This involves addressing the significant minority of respondents who expressed uncertainty or disagreement regarding the NIA's competence, benevolence, and integrity.

Finally, the research noted that though the sex bias in our data does not seem to impact the findings significantly, the education and age biases present a threat to their validity. Future research should aim to address these biases to provide a more representative understanding of public trust in the NIA. This will help ensure that the findings are more generalizable and reflective of the broader population.

Overall, this study contributes to the literature on trust in government-controlled organisations, particularly in the context of digitised identity systems. The insights gained from this research provide valuable guidance for the NIA and similar government agencies. By addressing the multifaceted dimensions of trust, including competence, benevolence, and integrity, these organisations can strengthen public trust and enhance the effectiveness of their information security policies. This, in turn, will help build a more secure and trusted digital identity system for the citizens of Ghana.

The next chapter will focus on discussion, and recommendations arising from bringing the four research studies together.

8 Conclusions

This chapter presents the main conclusions of the thesis, its contributions, and recommendations for practices, research, and further work. It further offers insights from the viewpoint of internal stakeholders (employees and management members) and external stakeholders (user agencies and the public).

8.1 Conclusions

The outcome of this research has significant implications for both the research community and EIS organisations by enhancing the ISP development, enforcement, and evolution processes. The findings from the four studies collectively highlight several key points.

Firstly, there is a consensus among all stakeholders on the necessity of a formally approved ISP and the importance of ISP awareness training. Employees recognised the NIA ISP's necessity, benefits, importance, and usefulness, feeling content, satisfied, accomplished, and fulfilled when complying with the ISP. This underscores the positive impact of a well-structured ISP on employee morale and compliance.

Secondly, the research revealed varying levels of awareness among staff about the NIA ISP provisions and the most common violations. While employees generally understood the ISP, there were differences in how well they could identify violations, indicating a need for more targeted training and communication.

Thirdly, the perceptions, knowledge, and understanding of stakeholders about IS effectiveness, IS management, and the formulation, expression, and evolution of the NIA ISP varied. Internal stakeholders, such as employees and management, emphasised the need for comprehensive IS education and effective enforcement mechanisms. External stakeholders, including user agencies and the public, highlighted the importance of transparency and trust in IS practices.

Areas of agreement among stakeholders include the recognition of the ISP's importance and the need for regular reviews and updates to address emerging security threats. There is also a shared understanding of the critical role of both human and technological strategies in ensuring ISP compliance.

However, there are areas of disagreement. For instance, internal stakeholders focused more on operational aspects, such as enforcement and compliance monitoring, while external stakeholders were more concerned with transparency and public engagement. These differences highlight the need for a balanced approach that addresses both internal and external perspectives.

In conclusion, the research underscores the importance of involving all relevant stakeholders in the ISP development and review processes. By addressing both areas of agreement and disagreement, NIA and other EIS organisations can develop more effective and comprehensive ISPs that meet the needs of all stakeholders.

8.2 Answer to Research Questions

To provide answers to the thesis research questions, the researcher adopted both qualitative and quantitative methods. The studies help us understand the situation with respect to the NIA and provide insights that can be generalised across different identity organisations.

8.2.1 Research Question 1: What do information security requirements of identity systems mean to the NIA information security policies?

The literature review revealed essential requirements for electronic identity systems, emphasising the importance of privacy, trustworthiness, confidentiality, integrity, and availability. The studies highlighted that NIA's IS requirements should include a formally approved ISP, comprehensive IS education, and effective monitoring and enforcement strategies.

8.2.2 Research Question 2: Should NIA ISP be expressed, formulated, and implemented differently?

The studies indicated that NIA ISP should be tailored to address the unique challenges of the organisation, including cultural and social factors. The ISP should incorporate both human and technological strategies, motivation, and punitive measures to ensure compliance.

8.2.3 Research Question 3: What internal and external factors affect the NIA ISP expression, formulation, and implementation?

Internal factors include motivation, knowledge, understanding, and compliance with the ISP, while external factors involve public expectations, trust, and stakeholder involvement. Key findings also highlighted government influence, public-private partnerships, and transparency towards external stakeholders.

8.3 Contributions

This thesis makes several contributions to the research community and the development, enactment, and evolution of Information Security Policies (ISP) within Electronic Identity Systems (EIS).

First, this research provides new insights into the perspectives of both internal and external stakeholders regarding their involvement in the development and evolution of ISPs in identity organisations. It highlights that all stakeholders, not just internal ones, strongly believe they should be involved in these processes. This finding underscores the importance of inclusive stakeholder engagement in ISP development.

Secondly, the study reveals that stakeholders have high expectations for information security management from identity organisations. This expectation extends beyond internal stakeholders to include external ones, emphasising the critical role of comprehensive security measures in maintaining trust and compliance.

Additionally, the research identifies that while the fundamental principles of information security are similar across different sectors, there is an increased emphasis on information security within identity organisations due to the significant impact of potential security breaches. This highlights the additional challenges faced by public sector organisations in managing information security.

From a methodological perspective, this thesis is the first to use a mixed-methods approach to study the development, enactment, and evolution of ISPs in an EIS organisation. As noted in Chapter 3, section 3.3.2, the use of mixed methods increases the validity of research findings and informs subsequent data collection, thereby enhancing the robustness of the conclusions. This approach provides a more useful insights into the issues by examining them from the perspectives of different stakeholders, which would not be possible through a single-method study.

Furthermore, the study confirms earlier findings about the importance of combining human and technological approaches to protect organisational data and systems. It also highlights the impact of motivation on ISP compliance and enforcement.

Finally, this thesis emphasises the necessity for both internal and external stakeholders in businesses, organisations, and governments to understand and comply with their ISPs. It underscores the importance of employee awareness and compliance in securing personal data and preventing organisational vulnerabilities. This research contributes to improving responsible behaviour among employees and other users, thereby enhancing the overall security posture of EIS organisations.

8.4 Recommendations for Practice

Research has shown that employees' attitudes and lack of security awareness are significant contributors to security incidents (Furnell, 2007). This study investigated the involvement of employees and other stakeholders in the development, enactment, and evolution processes of the NIA ISP. The findings highlight the importance of involving all relevant internal and external stakeholders in developing and regularly reviewing ISPs. However, the research results indicate that the NIA does not effectively involve all stakeholders.

For the NIA, it is crucial to develop a formally approved ISP to ensure clarity and consistency in information security practices. Regular intensive education and training for all stakeholders on their roles and responsibilities contained in the ISP are essential to protect data and systems effectively. Management buy-in and IS governance are also vital, as information security should be recognised as everyone's responsibility, with management playing a crucial role in fostering a culture of security awareness and accountability. Additionally, the NIA should enhance transparency with partners and the public to build trust, supported by literature on designing public services and public engagement. Effective management of external partner and supplier security is necessary, and adopting best practices such as those outlined by the National Cyber Security Centre (NCSC) on supply chain security and managing partner risk could be highly beneficial.

For other identity organisations, adopting best practices and international standards for information security management, ISP formulation, development, and evolution is recommended. Designing public services that include public engagement will ensure transparency and trust. Close collaboration with internal and external stakeholders is essential, emphasising the focus on people, including staff, partners, and the public, to avoid the mistakes identified in the NIA's approach. Regular reviews and updates of ISPs are necessary to reflect changes in the organisational environment and emerging security threats.

By implementing these recommendations, both the NIA and other identity organisations can enhance their information security practices, build trust with stakeholders, and ensure effective and efficient ISP formulation, evolution, and implementation processes.

8.5 Recommendations for Research

Based on the four studies, several areas for further research have been identified. One primary area is the examination of other organisations similar to the NIA. This includes investigating specific challenges in information security management and ISP formulation, development, and evolution within public sector organisations. Key issues that need further investigation include managing government interference, public-private partnerships, and public-sector staff management constraints. Additionally, there is a need to explore public engagement in building trustworthy public services. A complementary approach could involve document analysis, such as a comparative analysis of identity organisation ISPs with those of other organisations. Reviewing existing research on these topics can provide a starting point and early contributions to these issues.

Further comparative research could be conducted between the NIA and other similar EIS organisations in other developing countries to understand the differences and similarities in employee compliance frameworks. This research can use compliance factors such as content, readability, and comprehension metrics.

The COVID-19 pandemic influenced the timeframe for this research, highlighting the need for longer timeframes in future studies to incorporate unforeseen research-related occurrences.

More research is also required on the involvement of critical stakeholders in EIS ISP development, enactment, and evolution processes. Future studies could focus on actual NIA ISPs using document analysis or focused group discussions to provide deeper insights.

By addressing these areas and learning from the experiences of this research, future studies can build on the findings and contribute to a more comprehensive understanding of information security policies in digitised identity systems.

8.6 Challenges and Limitations

8.6.1 Challenges

This study encountered several key challenges and limitations that impacted the research process and findings. One significant challenge was the issue of incomplete responses, which led to some data being discarded due to failure to meet quality checks. This reduction in sample size potentially affected the representativeness of the data. To mitigate this, rigorous data quality checks were implemented, and a formula for selecting participants was used to maintain data integrity.

Another challenge was the threat to sample validity caused by the unavailability of some staff members due to the ongoing mass registration exercise or frequent travels for field operations. For instance, drivers deployed throughout the country were excluded from the research, which limited the diversity of perspectives. To address this, interviews and surveys were scheduled at times convenient for participants, and meeting venues were scheduled where possible.

The COVID-19 pandemic and subsequent lockdown restrictions significantly impacted the data collection process, causing delays and face-to-face interactions. Strict adherence to COVID-19 protocols ensured participant safety and continuity in data collection.

Financial constraints related to field operations, such as travel and accommodation costs, also posed challenges. Financial assistance from the department and personal resources from the researcher helped cover necessary expenses.

8.6.2 Limitations

Several limitations were noted in the study. The active involvement of the researcher, who had a past official role in the organisation, posed a threat to validity due to potential bias in data collection and analysis. Ethical standards were strictly followed, responses were anonymised, and multiple data sources were used to triangulate findings, mitigating this bias. The use of various tools, including manual questionnaires, audio recorders, semi-structured interview guides, and software like SPSS and NVIVO, introduced potential inconsistencies. Standardised data collection procedures and cross-checking of data helped ensure consistency.

The data collected within a specific timeframe may not reflect recent updates by the National Identification Authority (NIA), limiting the applicability of the findings. This limitation was acknowledged, and future studies were recommended to update the findings.

Participant withdrawal also reduced the sample size and potentially biased the results. Ensuring voluntary participation and providing flexible scheduling accommodated participants and mitigated this issue.

The limited research period prevented the researcher from conducting document analysis or focus group discussions, limiting the depth of qualitative insights. Future research was recommended to include these methods for a more comprehensive analysis. Additionally, the sensitivity of the data managed by respondents may have led to underreporting of issues and biased responses. Ensuring confidentiality and anonymity encouraged honest responses.

8.7 Future Work

This research is the first attempt to use the mixed method to conduct a Case study on the ISP trustworthiness, privacy and security requirements during the development, enforcement and evolution processes in an EIS digitised organisation; similar works can be conducted using a digitalised EIS.

In addition, the selected organisation is in a developing country, so similar research could be replicated in a developed economy or region to validate the generalisability of these findings.

As this research was focused on the Ghanaian EIS system, similar research can be conducted using other digitised systems, like the ones in Malawi, and Nigeria, among others, to validate this study's findings.

Again, a comparative study between other digitised versus digitalised EIS systems can be conducted in the future to enhance EIS ISP knowledge and understanding of their differences. Specific issues needing further investigation include managing government interference, public-private partnerships, and public-sector staff management constraints. Additionally, document analysis and focus groups involving different stakeholders could provide deeper insights.

References

Adams, A., & Sasse, M. A. (1999). Privacy in multimedia communications: Protecting users, not just data. In People and Computers XV—Interaction without Frontiers (pp. 49-64). Springer. https://doi.org/10.1007/978-1-4471-0353-0_4 accessed on 05/05/2025

African, U. (2020). The Digital Transformation Strategy for Africa (2020-2030). Retrieved from https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf accessed on 05/05/2025

AlHogail, A. (2015). Improving information security awareness in organizations: A review of literature. Journal of Theoretical and Applied Information Technology, 78(3), 456–471.

Aichholzer, G., & Strauß, S. (2010). The Austrian case: multi-card concept and the relationship between citizen ID and social security cards. Identity in the Information Society, 3(1), 65-85. Retrieved from https://link.springer.com/article/10.1007/s12394-010-0048-9 accessed on 06/05/2024

Ajzen, I. (1991). The theory of planned behaviour. Organisational Behaviour and Human Decision Processes, 50(2), 179-211. https://doi.org/10.1016/0749-5978(91)90020-T

Alassaf, M., & Alkhalifah, A. (2021). Exploring the influence of direct and indirect factors on information security policy compliance: A systematic literature review. IEEE Access, 9, 162687-162705. https://doi.org/10.1109/ACCESS.2021.3132574

Alkhurayyif, Y. A. (2019). Evaluating readability as a factor in information security policies (Doctoral dissertation, University of Strathclyde). Retrieved from https://stax.strath.ac.uk/concern/theses/vt150j43d accessed on 12/12/2024

Alkhurayyif, Y., & Weir, G. R. S. (2017). Evaluating readability as a factor in information security policies. International Journal of Trend in Research and Development, 4(2), 54-64. Retrieved from https://strathprints.strath.ac.uk/63070/ accessed on 12/12/2024

Alnatheer, M., & Nelson, K. J. (2009). A proposed framework for understanding information security culture and practices in the Saudi context. In C. Bolan (Ed.), Proceedings of the 7th Australian Information Security Management Conference (SECAU 2009) (pp. 1-12). Perth, Australia.

Alqahtani, F. H. (2017). Developing an information security policy: A case study approach. Procedia Computer Science, 124, 691-697. Accessed on 05/05/2024

Alshaikh, M., Chang, S., Ahmad, A., Maynard, S. B., & Alammary, A. (2022). Embedding information security management in organisations: improving participation and engagement through intra-organisational liaison. Security Journal, 36, 530-557. Accessed on 01/04/2024

Al-Wadi, M. (2009). Someone else conducting the same qualitative research at a different time could reveal something quite different. International Journal of Qualitative Studies in Education, 22(4), 389-403.

Allen, C. (2021). The path to self-sovereign identity. Journal of Digital Identity, 3(1), 1-15. Accessed on 05/09/2024

Alzahrani, L. (2018). "Factors Impacting Users' Compliance with Information Security Policies: An Empirical Study." Journal of Information Security and Applications, 42, 1-12 Accessed on 05/09/2024

American Psychological Association. (2001). Publication Manual of the American Psychological Association (5th ed.). Washington, DC: Author. https://psycnet.apa.org/record/2002-17725-000 Accessed on 05/02/2025

Ammann, F.-E., & Sowa, J. F. (2013). Information security management (ISM) practices: Lessons from select cases from India and Germany. Global Journal of Flexible Systems Management, 14(4), 241-255. https://doi.org/10.1007/s40171-013-0047-4 .

Anand, N., & Brass, I. (2021). Responsible innovation for digital identity systems. Data & Policy, 3, e35. https://doi.org/10.1017/dap.2021.35

Andress, J. (2014). The basics of information security: Understanding the fundamentals of InfoSec in theory and practice (2nd ed.). Syngress. https://doi.org/10.1016/C2013-0-18642-4

Anthopoulos, L. G., Siozos, P., & Tsoukalas, I. A. (2007). Applying participatory design and collaboration in digital public services for discovering and re-designing e-Government services. Government Information Quarterly, 24(2), 353-376. https://doi.org/10.1016/j.giq.2006.07.018

Ansoff, H. I. (1965). Corporate Strategy. New York, McGraw-Hill. Ansoff, HI (1965b) Strategic Management,(2), 471-517. Accessed on 04/05/2023

Arthi, M. C., & Shanmugam, K. (2023). Implementing unique identification technology: The journey and success story of Aadhaar in India. Journal of Information Technology Teaching Cases, 14(2), 241-246.https://doi.org/10.1177/20438869231200286

Atick, J. (2016). Digital identity: the essential guide. In ID4Africa Identity Forum (Vol. 2016, pp. 1-3). Accessed on 04/06/2024

Aurigemma, S., & Mattson, T. (2019). Generally speaking, context matters: Making the case for a change from universal to particular ISP research. Journal of the Association for Information Systems, 20(12), 7. Accessed on 04/05/2024

Azeem, M., Salfi, N. A., & Dogar, A. (2012). Usage of NVivo software for qualitative data analysis. Academic Research International, 2(1), 262-266.

Babbie, E. R. (2016). The practice of social research (14th ed.). Cengage Learning. https://www.scirp.org/reference/referencespapers?referenceid=2439585 accessed on 10/05/2025.

Bachmann, R. (2011). At the crossroads: Future directions in trust research. Journal of Trust Research, 1(2), 203-213. DOI: 10.1080/21515581.2011.603513

Bamaga, A., Terzis, S., & Zafar, B. (2024). Quality factors impacting e-learning within the mobile environment in Saudi Arabia universities: An interview study. International Journal of Data and Network Science, 8(1), 269-288. https://doi.org/10.5267/j.ijdns.2023.9.025

Bannister, F., & Connolly, R. (2011). Trust and transformational government: A proposed framework for research. Government Information Quarterly, 28(2), 137–147. https://doi.org/10.1016/j.giq.2010.06.010

Baskerville, R. (1993). Information systems security design methods: implications for information systems development. ACM Computing Surveys (CSUR), 25(4), 375-414. https://doi.org/10.1145/162124.162127

Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organisations. Logistics Information Management, 15(5/6), 337-346.

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. Information & Management, 51(1), 138-151. https://doi.org/10.1016/j.im.2013.11.004

BECTA. (2001, 2009). Acceptable Use Policy. British Educational Communications and Technology Agency. Retrieved from https://www.safeguardingcambspeterborough.org.uk/wpcontent/uploads/2014/06/BECTA_AUP_Guidance.pdf. Accessed on 15/03/2025

Belanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. Information & Management, 54(7), 887-901.

Bell, J. (1984). Doing your research project: A guide for first-time researchers in education and social science. Open University Press.

Berg, B. L. (2001). Qualitative research methods for the social sciences (4th ed.). Allyn & Bacon.

Beck-Krala, E. (2020). Rewards effectiveness. In Encyclopedia of Sustainable Management. SpringerLink. https://link.springer.com/referenceworkentry/10.1007/978-3-030-02006-4_213-1 accessed on 14/05/2025

Björck, F. (2001). Implementing Information Security Management Systems: An Empirical Study of Critical Success Factors. Advances in Information Security Management & Small Systems Security, 197-211.

Blaikie, N. (2003). Analyzing quantitative data: From description to explanation. SAGE Publications. Retrieved from https://books.google.co.uk/books?hl=en&lr=&id=sNQ54wUa2SwC&oi=fnd&pg=PP2&ots=varZpHcYO&sig=DRZVutuEjmrQv0ZglG6t60DuWQU&redir_esc=y#v=onepage&q&f=false

Blakley, B., McDermott, E., & Geer, D. (2002). Information management is information risk management. In Proceedings of the 2001 Workshop on New Security Paradigms (NSPW 2001), pp. 97–104. ACM. http://nspw.org/papers/2001/nspw2001-blakley.pdf.

Bouckaert, G., & Van de Walle, S. (2003). Comparing measures of citizen trust and user satisfaction as indicators of 'good governance': Difficulties in linking trust and satisfaction indicators. International Review of Administrative Sciences, 69(3), 329-343.

Boss, S. R., & Kirsch, L. J. (2007). The last line of defense: Motivating employees to follow corporate security guidelines. ICIS 2007 Proceedings, 122.

Boyatzis, R. E. (1998). Transforming qualitative information: Thematic analysis and code development. SAGE Publications.

Brancheau, J. C., Janz, B. D., & Wetherbe, J. C. (1996). Key issues in information systems management: 1994-95 SIM Delphi results. MIS Quarterly, 20(2), 225-242.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77-101.

Briggs, A. R. J., Coleman, M., & Morrison, M. (2012). Research methods in educational leadership and management (3rd ed.). SAGE Publications.

Bryman, A. (2012). Social research methods (4th ed.). Oxford University Press. https://books.google.com/books/about/Social_Research_Methods.html?id=vCq5m2hPkOMC.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523-548.

Cahill et al. (2003). Using trust for secure collaboration in uncertain environments. IEEE Pervasive Computing, 2(3), 52-61. https://doi.org/10.1109/MPRV.2003.1228527.

California Legislature. (2018). California Consumer Privacy Act of 2018. Retrieved from https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375 accessed on 05/06/2025

Campbell, D. T., & Fiske, D. W. (1959). Convergent and discriminant validation by the multitrait-multimethod matrix. Psychological Bulletin, 56(2), 81-105.

Canavan, S. (2003). An information security policy development guide for large companies. Sans Institute.

Carr, W. (1994). The small selective sample size is related to the in-depth nature of the qualitative approach. Journal of Qualitative Research, 12(3), 45

Cavoukian, A. (2011). Privacy by Design: The 7 Foundational Principles. Information and Privacy Commissioner of Ontario, Canada. Retrieved from https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2022). Developing metrics to assess the effectiveness of cybersecurity awareness program. Journal of Cybersecurity, 8(1), tyac006.

Chen, H., & Li, W. (2014). Understanding organisation employee's information security omission behaviour: An integrated model of social norm and deterrence. Paper presented at the Pacific Asia Conference on Information Systems (PACIS). https://aisel.aisnet.org/pacis2014/280/.

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2012). Organisations' information security policy compliance: Stick or carrot approach? Journal of Management Information Systems, 29(3), 157-188.

Choudhury, V., & Sabherwal, R. (2003). Portfolios of control in outsourced software development projects. Information Systems Research, 14(3), 291-314.

Churchill, G. A. (1979). A paradigm for developing better measures of marketing constructs. Journal of Marketing Research, 16(1), 64-73.

Claburn, T. (2018b). British Airways breach: 380,000 card payments 'compromised'. The Register. Retrieved from https://www.theregister.com/2018/09/06/british_airways_breach/ accessed on 09/09/2018

Clark, M. C., & Payne, R. L. (1997). The nature and structure of workers' trust in management. Journal of Organisational Behaviour: The International Journal of Industrial, Occupational and Organisational Psychology and Behaviour, 18(3), 205-224.

Clegg, F. (1998). Simple statistics: A course book for the social sciences. Cambridge University Press. https://books.google.com/books/about/Simple_Statistics.html?id=v9hiQgAACAAJ

Cofta, P. (2008). Towards a better citizen identification system. Identity in the Information society, 1(1), 39-53.

Cohen, L., Manion, L., & Morrison, K. (2000). Research methods in education (5th ed.). Routledge. https://doi.org/10.4324/9781315456539

Cohen, L., Manion, L., & Morrison, K. (2007). Qualitative data analysis involves organising, accounting for and explaining the data; in short, making sense of data in terms of the participants' definitions of the situation, noting patterns, themes, categories and regularities. In Research Methods in Education (6th ed.). Routledge. https://doi.org/10.4324/9780203029053.

Cohen, L., Manion, L., & Morrison, K. (2011). Research methods in education (7th ed.). Routledge.

Collaboration on International ICT Policy for East and Southern Africa (CIPESA). (2022). Data Governance and Public Trust: Exploring the Sources of Low Trust Levels in Public Data Controllers in Ghana. Retrieved from https://africaportal.org/wp-content/uploads/2023/06/Ghana-report.pdf

Coles-Kemp, L. (2009). Information security management: An entangled research challenge. Information Security Technical Report, 14(4), 181-185.

Colwill, C. (2009). Human factors in information security: The insider threat–Who can you trust these days? Information Security Technical Report, 14(4), 186-196.

Corrocher, N., & Ordanini, A. (2002). Measuring the digital divide: A framework for the analysis of cross-country differences. Journal of Information Technology, 17, 9-19.

Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? New Media & Society, 21(10), 2305-2322.

Coyle, A., & Williams, B. (2000). An exploration of the epistemological intricacies of mixed-method research. Journal of Mixed Methods Research, 4(2), 123-134.

Cram, W. A., Brohman, K., & Gallupe, R. B. (2016). Information systems control: A review and framework for emerging information systems processes. Journal of the Association for Information Systems, 17(4), 2.

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organisational information security policies: A review and research framework. European Journal of Information Systems, 26(6), 605-641. https://doi.org/10.1057/s41303-017-0059-9

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. Psychometrika, 16(3), 297-334.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioural information security research. Computers & Security, 32, 90-101.

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. The TQM Journal, 33(7), 76-105.

Cushman, J. E., Kelly, M. R., Fusco-Rollins, M., & Faulkner, R. (2021). Using Qualtrics Core XM for surveying youth. Journal of Youth Development, 16(1). https://doi.org/10.5195/jyd.2021.886

Cummings, L. L., & Bromiley, P. (1996). The Organizational Trust Inventory (OTI): Development and validation. In R. M. Kramer & T. R. Tyler (Eds.), Trust in organizations: Frontiers of theory and research (pp. 302–330). SAGE Publications. https://doi.org/10.4135/9781452243610.n15.

Da Veiga, A. (2018). An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture. Information and Computer Security, 26(5), 584-612. https://doi.org/10.1108/ICS-08-2017-0056

Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. Computers & Security, 29(2), 196-207.

D’Arcy, J., & Hovav, A. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Information Systems Research, 20(1), 79-98. https://doi.org/10.1287/isre.1070.0160

David, J. (2002). Policy enforcement in the workplace. Computers & Security, 21(6), 506-513.

Davis, G. B., & Olson, M. H. (1984). Management information systems: Conceptual foundations, structure, and development. McGraw-Hill, Inc.

Dehaene, S., & Mehler, J. (1990). Cross-linguistic regularities in the frequency of number words. Cognition, 37(1), 93-97.

Dehaene, S., Bossini, S., & Giraux, P. (1993). The mental representation of parity and number magnitude. Journal of Experimental Psychology: General, 122(3), 371-396.

De Leeuw, E. D., Hox, J. J., & Dillman, D. A. (2012). International handbook of survey methodology. Routledge. https://doi.org/10.4324/9780203843123.

Denzin, N. K., & Lincoln, Y. S. (1998). The landscape of qualitative research: Theories and issues. SAGE Publications.

https://books.google.com/books/about/The_Landscape_of_Qualitative_Research.html?id=Sxa2AAAAIAAJ.

Denning, D. E. (1999). Information warfare and security. ACM Press. Retrieved from https://link.springer.com/content/pdf/10.1023/A:1010081405155.pdf

Desselle, S. P. (2005). Construction, implementation, and analysis of summated rating attitude scales. American Journal of Pharmaceutical Education, 69(5), 1-11.

Dhillon, G., & Backhouse, J. (2000a). Technical opinion: Information system security management in the new millennium. Communications of the ACM, 43(7), 125-128. https://doi.org/10.1145/341852.341877

Diver, S. (2007). Information security policy–a development guide for large and small companies. Sans Institute, 1-37.

Doherty, N. F., & Fulford, H. (2005). Do information security policies reduce the incidence of security breaches: An exploratory analysis. Information Resources Management Journal (IRMJ), 18(4), 21-39.

Doherty, N. F., & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. Computers & Security, 25(1), 55-63.

Doherty, N. F., Anastasakis, L., & Fulford, H. (2009). The information security policy unpacked: A critical study of the content of university policies. International Journal of Information Management, 29(6), 449-457.

Duodu, E. E. (2018). Implementation of a national identification system in Ghana: Lessons from the Indian Aadhaar system. University of Ghana. Retrieved from https://ugspace.ug.edu.gh/bitstreams/5bc91e5b-c53e-4dad-9a39-56f0089ab2b8/download.

Edu, J., Hooper, M., Maple, C., & Crowcroft, J. (2023, June). An impact and risk assessment framework for national electronic identity (eID) systems. In International Conference on AI and the Digital Economy (CADE 2023) (Vol. 2023, pp. 124-133). IET.

Equality and Human Rights Commission. (2021). Your rights to equality and human rights. Retrieved from https://www.equalityhumanrights.com/en/human-rights/what-are-human-rights accessed on 09/09/2024

Ernst & Young. (2008). Moving beyond compliance: Ernst & Young’s 2008 Global Information Security Survey. Retrieved from http//www.ey.com/Publication/vwLUAssets/2008_Global_Information_Security_Survey_english/$FILE/20 08_GISS_ingles.pdf).

EU Federal Chancellery. (2020). Digital sovereignty: Insights from Germany's education sector. Erstelesung. Retrieved from https://publishup.uni-potsdam.de/opus4-ubp/files/59772/tbhpi157.pdf

European Union. (2016). General Data Protection Regulation (GDPR). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj Accessed on 05/06/2025

Farooq, A., Isoaho, J., Virtanen, S., & Isoaho, J. (2015). Information security awareness in educational institution: An analysis of students' individual factors. Paper presented at the 2015 IEEE Trustcom/BigDataSE/ISPA. Retrieved from https://doi.org/10.1109/Trustcom.2015.394.

Farooq, A., Kakakhel, S. R. U., Virtanen, S., & Isoaho, J. (2015). A taxonomy of perceived information security and privacy threats among IT security students. Paper presented at the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). Retrieved from https://www.utupub.fi/bitstream/handle/10024/156706/Paper%20ID%20144_Camera%20Ready.pdf?sequence=1.

Florêncio, D., & Herley, C. (2010). A large-scale study of web password habits. Proceedings of the 19th International Conference on World Wide Web, 657-666. https://doi.org/10.1145/1772690.1772758

Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. Computers & Security, 61, 169-183.

Furnell, S. (2007). Cybercrime: Vandalizing the information society. Springer. https://doi.org/10.1007/3-540-45068-8_2

Furnell, S., Sohrabi Safa, N., & Von Solms, R. (2016). Information security policy compliance model in organisations. Computers & Security, 56, 1-13. https://doi.org/10.1016/j.cose.2015.10.006

Fussell, J. (2001). Group classification on national ID cards as a factor in genocide and ethnic cleansing. Paper presented at the Seminar Series of the Yale University Genocide Studies Programme, New Haven. Retrieved from https://www.academia.edu/52172135/Group_classification_on_national_ID_cards_as_a_factor_in_genocide_and_ethnic_cleansing.

Galvin, J. (1999). Writing literature reviews: A guide for students of the social and behavioural sciences. Los Angeles: Pyrczak Publishing. Retrieved from https://archive.org/details/writingliteratur0000galv_l1l7.

Gambetta, D. (1988), Trust: Making and Breaking Cooperative Relations, Basil Blackwell, Oxford, pp213-238

Gelb, A., & Clark, J. (2013). Identification for Development: The Biometrics Revolution. Center for Global Development. https://documents1.worldbank.org/curated/en/566431581578116247/pdf/Identification-for-Development-ID4D-2019-Annual-Report.pdf

Geisler, S., Vidal, M.-E., Cappiello, C., Lóscio, B. F., Gal, A., Jarke, M., … Paja, E. (2021). Knowledge-driven data ecosystems toward data transparency. ACM Journal of Data and Information Quality (JDIQ), 14(1), 1-12.

Ghosh, S. (2016). How important is mobile telephony for economic growth? Evidence from MENA countries. Digital Policy, Regulation and Governance, 18(3), 58–79. Retrieved from https://doi.org/10.1108/info-12-2015-0058.

Gillespie, N. (2003). Measuring trust in working relationships: The behavioural trust inventory. Melbourne Business School. Retrieved from https://www.econbiz.de/Record/measuring-trust-in-working-relationships-the-behavioral-trust-inventory-gillespie/10001769936.

Glassner, B., & Moreno, J. D. (2013). The qualitative-quantitative distinction in the social sciences. Springer. Retrieved from https://link.springer.com/book/10.1007/978-94-017-3444-8.

Glöckler, J., Sedlmeir, J., Frank, M., & Fridgen, G. (2024). A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity. Business & Information Systems Engineering, 66(4), 421-440.

Godefroidt, A., Langer, A., & Meuleman, B. (2017). Developing political trust in a developing country: The impact of institutional and cultural factors on political trust in Ghana. Democratization, 24(6), 906-928.

Goel, S., & Chengalur-Smith, I. N. (2010). Metrics for characterising the form of security policies. The Journal of Strategic Information Systems, 19(4), 281-295.

Gollmann, D. (2010). Computer security. John Wiley & Sons. Retrieved from https://books.google.com/books/about/Computer_Security.html?id=KTYxTfyjiOQC.

Government of Canada. (2000). Personal Information Protection and Electronic Documents Act (PIPEDA). Retrieved from https://laws-lois.justice.gc.ca/eng/acts/P-8.6/ accessed on 06/05/2025

Granovetter, M. (1985). Economic action and social structure: The problem of embeddedness. American Journal of Sociology, 91(3), 481-510.

Grant, J. A. (2011). The national strategy for trusted identities in cyberspace: Enhancing online choice, efficiency, security, and privacy through standards. IEEE Internet Computing, 15(6), 80-84.

Gray, D. E. (2013). Doing research in the real world (3rd ed.). SAGE Publications. Retrieved from https://uk.sagepub.com/en-gb/eur/doing-research-in-the-real-world/book275378.

Greenleaf, G. (2010). India's national ID system: Danger grows in a privacy vacuum. Computer Law & Security Review, 26(5), 479-491.

Grimmelikhuijsen, S., & Knies, E. (2017). Validating a scale for citizen trust in government organisations. International Review of Administrative Sciences, 83(3), 583-601.

Grönlund, Å. (2001). Introducing e-Gov: History, definitions, and issues. Örebro University. Retrieved from https://www.researchgate.net/publication/234008823_Introducing_e-Gov_History_Definitions_and_Issues

Gukurume, S., & Mahiya, I. T. (2020). Mobile money and the (un) making of social relations in Chivi, Zimbabwe. Journal of Southern African Studies, 46(6), 1203-1217.

Guo, K. H. (2013). Security-related behaviour in using information systems in the workplace: A review and synthesis. Computers & Security, 32, 242-251.

Haaker, M. (2019). Causal-correlational designs. In P. Atkinson, S. Delamont, A. Cernat, J. W. Sakshaug, & R. A. Williams (Eds.), SAGE Research Methods Foundations. SAGE Publications Ltd. https://doi.org/10.4135/9781526421036849600

Hair Jr, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1998). Multivariate data analysis 5th ed Prentice Hall Upper Saddle River. NJ. Retrieved from https://www. scirp. org/(S (351jmbntvnsjt1aadkpo szje))/reference/ReferencesPapers. aspx.

Halperin, R., & Backhouse, J. (2012). Risk, trust and eID: Exploring public perceptions of digital identity systems. First Monday, 17(4).

Hancock, D. R., & Algozzine, B. (2016). Doing case study research: A practical guide for beginning researchers (2nd ed.). Teachers College Press.

Handforth, C. W., Matthew. (2019). Digital identity country report: Malawi, 1-20. Retrieved from https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/Digital-Identity-Country-Report.pdf

Hardin, R. (2002). Trust and trustworthiness. Russell Sage Foundation. Retrieved from https://www.russellsage.org/publications/trust-and-trustworthiness-1.

Harris, S. (2017). CISSP All-in-One Exam Guide (8th ed.). McGraw-Hill Education. Retrieved from https://books.google.com/books/about/CISSP_All_in_One_Exam_Guide_Eighth_Editi.html?id=5StxDwAAQBAJ.

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

Herath, T. B., Khanna, P., & Ahmed, M. (2022). Cybersecurity practices for social media users: A systematic literature review. Journal of Cybersecurity and Privacy, 2(1), 1-18.

Higgins, S. (1999). Information security policies: A content analysis. Springer. https://link.springer.com/chapter/10.1007/978-3-319-31232-3_46

Holbert, C. (2013). Sample size determination for correlation studies. Retrieved from https://www.cfholbert.com/blog/sample-size-correlation/ accessed on 23/07/2022.

HöNe, K., & Eloff, J. (2002). What makes an effective information security policy? Network Security, 2002(6), 14-16.

Hong, K. S., Chi, Y. P., Chao, L. R., & Tang, J. H. (2006). An empirical study of information security policy on information security elevation in Taiwan. Information Management & Computer Security, 14(2), 104-115.

https://joinup.ec.europa.eu/collection/riha-estonian-catalogue-public-sector-information-systems (accessed on 08/09/2024)

Hurmerinta-Peltomaki, L., & Nummela, N. (2006). Mixed methods in international business research: A value-added perspective. Management International Review, 46(4), 439-459.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behaviour and the protection motivation theory. Computers & Security, 31(1), 83-95.

Information Commissioner's Office. (2023). Guide to the UK General Data Protection Regulation (UK GDPR). https://ico.org.uk/for-organisations/uk-gdpr-guidance/ accessed on 11/06/2025

Information System Authority. (2018). Retrieved from https://www.ria.ee/en/media/1506/download.

Information System Authority. (2018). Retrieved from https://www.ria.ee/en.html.

Information System Authority. (2019). Retrieved from https://www.ria.ee/media/1502/download.

International Organisation for Standardisation. (2013). ISO/IEC 27001: 2013: Information technology–Security techniques–Information security management systems–Requirements. International Organisation for Standardisation. https://www.iso.org/standard/54533.html

International Organisation for Standardisation. (2024). ISO/IEC 27000 family — Information security management. Retrieved from https://www.iso.org/standard/iso-iec-27000-family accessed on 09/09/2024

International Organisation for Standardisation. (2021). ISO/IEC 27001: 2021 — Monitoring Efficacy & Continuous Improvement. Retrieved from https://www.standardfusion.com/blog/guide-to-iso-27001-monitoring-efficacy-and-continuous-improvement/ accessed on 09/09/2024

ISACA. (2009). The risk IT framework. ISACA. https://books.google.com/books/about/The_Risk_IT_Framework.html?id=tG7VMihmwtsC.

Jai-Yeol, S. (2011). Information security management and compliance: A socio-technical perspective. Journal of Information Systems, 25(1), 1-24. https://doi.org/10.2308/jis.2011.25.1.1

Jamieson, S. (2004). Likert scales: How to (ab)use them. Medical Education, 38(12), 1217-1218. https://doi.org/10.1111/j.1365-2929.2004.02012.x

Janssens, W., Wijnen, K., De Pelsmacker, P., & Van Kenhove, P. (2008). Marketing research with SPSS. Pearson Education; Financial Times; Prentice Hall. https://books.google.com/books/about/Marketing_Research_with_SPSS.html?id=N5KBEfab9TQC.

Johnson, E. C. (2006). Security awareness: Switch to a better programme. Network Security, 2, 15-18.

Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. (2016). Dispositional and situational factors: Influences on information security policy violations. European Journal of Information Systems, 25(3), 231-251.

Jones, H. S., & Moncur, W. (2020). A mixed-methods approach to understanding funder trust and due diligence processes in online crowdfunding investment. ACM Transactions on Social Computing, 3(1), 1-29.

Just, M., & Renaud, K. (2012). Trends in Government e-Authentication: Policy and Practice. In Digital Democracy: Concepts, Methodologies, Tools, and Applications (pp. 1792-1805): IGI Global.

Jyoti, B. (2016). SPSS as a means for scientific analysis in social science research. International Journal of Innovative Technology and Exploring Engineering, 8(12), 1-5. Retrieved from https://www.ijitee.org/wp-content/uploads/papers/v8i12/L32521081219.pdf

Kalvet, T. (2012). Innovation: A factor explaining e-government success in Estonia. Electronic Government, an International Journal, 9(2), 142-157.

Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. International Journal of Information Management, 23(2), 139-154.

Karlsson, F., Åström, J., & Karlsson, M. (2015). Information security culture–state-of-the-art review between 2000 and 2013. Information & Computer Security, 23(3), 246-285.

Karlsson, F., Hedström, K., & Goldkuhl, G. (2017). Practice-based discourse analysis of information security policies. Computers & Security, 67, 267-279.

Karlsson, F., Kolkowska, E., & Prenkert, F. (2016). Inter-organisational information security: A systematic literature review. Information & Computer Security, 24(5), 418-451.

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: A contextual perspective. Computers & Security, 24(3), 246-260.

Kelle, U. (1997a). Computer-aided qualitative data analysis: Theory, methods and practice. SAGE Publications. https://uk.sagepub.com/en-gb/eur/computer-aided-qualitative-data-analysis/book204361.

Kelle, U. (1997b). Theory building in qualitative research and computer programs for the management of textual data. Sociological Research Online, 2(2), 10-22.

Kelley, K., Clark, B., Brown, V., & Sitzia, J. (2003). Good practice in the conduct and reporting of survey research. International Journal for Quality in Health Care, 15(3), 261-266.

Kiel, J. M., Ciamacco, F. A., & Steines, B. T. (2016). Privacy and data security: HIPAA and HITECH. In Healthcare Information Management Systems (pp. 437-449). Springer.

King, N. J., & Raja, V. (2012). Protecting the privacy and security of sensitive customer data in the cloud. Computer Law & Security Review, 28(3), 308-319.

Kinnunen, H., & Siponen, M. T. (2018). Developing organisation-specific information security policies. PACIS, 2018, 1-13.

Kirsch, L., & Boss, S. (2007). The last line of defense: Motivating employees to follow corporate security guidelines. ICIS 2007 Proceedings, 103.

Knapp, K. J., & Ferrante, C. J. (2012). Policy awareness, enforcement and maintenance: Critical to information security effectiveness in organisations. Journal of Management Policy and Practice, 13(5), 66-80.

Knapp, K. J., Morris Jr, R. F., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organisational-level process model. Computers & Security, 28(7), 493-508.

Knapp, T. R. (1990). Treating ordinal scales as interval scales: An attempt to resolve the controversy. Nursing Research, 39(2), 121-123. https://doi.org/10.1097/00006199-199003000-00019

Koops, B.-J. (2014). The trouble with European data protection law. International Data Privacy Law, 4(4), 250-261.

Krueger, R. A. (1998). Analysing & reporting focus group results. SAGE Publications. https://us.sagepub.com/en-us/nam/analyzing-and-reporting-focus-group-results/book6630

Kubicek, H., & Noack, T. (2010). Different countries-different paths extended comparison of the introduction of eIDs in eight European countries. Identity in the Information Society, 3(1), 235-245.

Kukutai, T., & Taylor, J. (2016). Indigenous data sovereignty: Toward an agenda. ANU Press. https://press.anu.edu.au/publications/series/caepr/indigenous-data-sovereignty.

Kulyk, O., Renaud, K., & Costica, S. (2023). People want reassurance when making privacy-related decisions - not technicalities. The Journal of Systems & Software, 200, 111620.

Kunz, S., Fabian, B., Marx, D., & Müller, S. (2011). Engineering policies for secure interorganisational information flow. Paper presented at the 2011 IEEE 15th International Enterprise Distributed Object Computing Conference Workshops.

Kwame Adjei, J. (2013). Towards a trusted national identities framework. Info, 15(1), 48-60.

Lampson, B. W. (2004). Computer security in the real world. Computer, 37(6), 37-46.

Landoll, D. (2016). Information security policies, procedures, and standards: A practitioner's reference. Auerbach Publications. https://doi.org/10.1201/9781315372785.

Lapke, M. S. (2008). Power relationships in information systems security policy formulation and implementation. https://aisel.aisnet.org/ecis2008/119/.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behaviour: A theory-based literature review. Management Research Review, 37(12), 1049-1092.

Lewis, P., & Baker, S. (2013). Information security policy compliance: An organisational perspective. Journal of Information Security, 4(2), 123-145.

Leyden, J. (2017, March 28). Gemalto releases findings of 2016 Breach Level Index. The Register. Retrieved from https://www.theregister.com/2017/03/28/gemalto_releases_findings_of_2016_breach_level_index/ accessed on 10/10/2018

Liang, J., Krause, N. M., & Bennett, J. M. (2001). Social exchange and well-being: Is giving better than receiving? Psychology and Aging, 16(3), 511.

Likert, R. (1932). A technique for the measurement of attitudes. Archives of Psychology, 22(140), 55.

Lohmeyer, D., McCrory, J., & Pogreb, S. (2002). Managing information security: Protecting the enterprise and its assets. McKinsey Quarterly. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Managing%20information%20security/Managing%20information%20security.pdf.

Loo, W. H., Yeow, P. H. P., & Chong, S. C. C. (2011). Acceptability of multipurpose smart national identity card: An empirical study. Journal of Global Information Technology Management, 14(1), 35–58. https://doi.org/10.1080/1097198X.2011.10856530

Lopes, I. M., & Sá-Soares, F. D. (2012). Information security policies: A content analysis. In PACIS-The Pacific Asia Conference on Information Systems. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1193&context=pacis2012.

Lowry, P. B., & Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. Information Systems Journal, 25(5), 433-463.

Lusoli, W., & Miltgen, C. (2009). Young people and emerging digital services: An exploratory survey on motivations, perceptions and acceptance of risks. European Commission Joint Research Centre. Retrieved from https://publications.jrc.ec.europa.eu/repository/bitstream/JRC50089/jrc50089.pdf

Lyon, D., & Bennett, C. J. (2008). Playing the ID card: Understanding the significance of identity card systems. In Playing the identity card: Surveillance, security and identification in global perspective (pp. 3-20).

Madianou, M. (2019). Technocolonialism: Digital innovation and data practices in the humanitarian response to refugee crises. Social media + Society, 5(3), 1–13. https://doi.org/10.1177/2056305119863146

Madise, Ü., & Martens, T. (2006). E-voting in Estonia 2005: The first practice of country-wide binding Internet voting in the world. In Electronic Voting 2006 – 2nd International Workshop (pp. 15-26). Bonn: Gesellschaft für Informatik e.V. Retrieved from https://dl.gi.de/items/b15050c3-a8ea-46f9-8976-1584b3cf499f.

Mason, J. (2002). Qualitative researching. Sage Publications.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. Academy of Management Review, 20(3), 709-734.

Mayer, R. C., & Davis, J. H. (1999). The effect of the performance appraisal system on trust for management: A field quasi-experiment. Journal of Applied Psychology, 84(1), 123.

Maynard, S. B., Ruighaver, A. B., & Ahmad, A. (2011). Stakeholders in security policy development. In Proceedings of the 9th Australian Information Security Management Conference (pp. 125-135). Edith Cowan University

McAllister, D. J. (1995). Affect-and cognition-based trust as foundations for interpersonal cooperation in organisations. Academy of Management Journal, 38(1), 24-59.

McCall, R., Baillie, L., Boehm, F., & Just, J. (2012). Workshop on: exploring the challenges of ethics, privacy and trust in serious gaming. Paper presented at the International Conference on Entertainment Computing. Retrieved from https://link.springer.com/referenceworkentry/10.1007/978-981-4560-50-4_37.

McEvily, B., & Tortoriello, M. (2011). Measuring trust in organisational research: Review and recommendations. Journal of Trust Research, 1(1), 23-63.

McKnight, D. H., & Chervany, N. L. (1996). The meanings of trust. MIS Research Center Working Papers, 96(04). Retrieved from https://home.nr.no/~abie/Papers/TheMeaningOfTrust.pdf.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. Information Systems Research, 13(3), 334-359.

Meade, A. W., & Craig, S. B. (2012). Identifying careless responses in survey data. Psychological Methods, 17(3), 437-455. https://doi.org/10.1037/a0028085

Merriam, S. B. (2001). Qualitative research and case study applications in education. Jossey-Bass.

Merriam, S. B., & Tisdell, E. J. (2016). Designing your study and selecting a sample. In Qualitative research: A guide to design and implementation (pp. 67-104).

Mikuletič, S., Vrhovec, S., Skela-Savič, B., & Žvanut, B. (2024). Security and privacy oriented information security culture (ISC): Explaining unauthorised access to healthcare data by nursing employees. Computers & Security, 136, 103489.

Miles, M. B., & Huberman, A. M. (1994). Qualitative data analysis: An expanded sourcebook (2nd ed.). SAGE Publications. Retrieved from Google Books: https://books.google.com/books/about/Qualitative_Data_Analysis.html?id=U4lU_-wJ5QEC.

Mingers, J. (2003). The paucity of multimethod research: A review of the information systems literature. Information Systems Journal, 13(3), 233-249.

MobiLoud. (2024). eCommerce market size by country [Updated 2024]. Retrieved from https://www.mobiloud.com/blog/ecommerce-market-size-by-country (accessed on 09/09/2024)

Molina-Azorin, J. F. (2011). The use and added value of mixed methods in management research. Journal of Mixed Methods Research, 5(1), 7-24.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. MIS Quarterly, 42(1), 285-311.

Morse, J. M., & Chung, S. E. (2003). Toward holism: The significance of combining qualitative and quantitative methods in research. Qualitative Health Research, 13(6), 733-743.

Morse, J. M., & Richards, L. (2002). Readme first for a user's guide to qualitative methods. SAGE Publications. Retrieved from Google Books: https://books.google.com/books/about/README_FIRST_for_a_User_s_Guide_to_Quali.html?id=G39Aff1cC7cC.

Nardi, P. M. (2015). Doing survey research: A guide to quantitative methods (4th ed.). Routledge. Retrieved from Taylor & Francis: https://www.taylorfrancis.com/books/mono/10.4324/9781315172231/survey-research-peter-nardi.

Nash, K., & Greenwood, D. (2008). The global state of information security. CIO Magazine, 6. Retrieved from https://www.csoonline.com/article/522546/the-global-state-of-information-security-2008.html.

National Academy of Public Administration. (1999). A government to trust and respect: Rebuilding citizen-government relations for the 21st century: A report. National Academy of Public Administration. Retrieved from HathiTrust Digital Library: https://catalog.hathitrust.org/Record/007988020.

National Institute of Standards and Technology. (2013). Security and privacy controls for federal information systems and organisations (NIST SP 800-53 Rev. 4). https://doi.org/10.6028/NIST.SP.800-53r4

Government of Ghana. (2006). National Identification Authority Act, Act 707. Parliament of the Republic of Ghana, Accra, Ghana. Retrieved from Parliament of Ghana: https://ir.parliament.gh/bitstream/handle/123456789/1937/NATIONAL%20IDENTIFICATION%20AUTHORITY%20ACT,%202006%20%28ACT%20707%29.pdf.

Neuman, W. L. (2013). Social research methods: Qualitative and quantitative approaches (7th ed.). Pearson Education. Retrieved from Google Books: https://books.google.com/books/about/Social_Research_Methods.html?id=Ybn3ngEACAAJ.

Nicoletta, M., & Andrea, P. (2002). Transformative impacts of information systems on society. Information Society Journal, 18(3), 201-220.

Niemimaa, E., & Niemimaa, M. (2017). Information systems security policy implementation in practice: From best practices to situated practices. European Journal of Information Systems, 26(1), 1-20.

Niemimaa, M., Laaksonen, A. E., & Harnesk, D. (2013). Interpreting information security policy outcomes: A frames of reference perspective. Paper presented at the 2013 46th Hawaii International Conference on System Sciences.

Nurse, J. R. C., Creese, S., Goldsmith, M., & Lamberts, K. (2014). Trustworthy and effective communication of cybersecurity risks: A review. Human Aspects of Information Security, Privacy, and Trust, 1-10.

Nunnally, J. C., & Bernstein, I. H. (1994). Psychometric theory (3rd ed.). McGraw-Hill. Retrieved from Open Library: https://openlibrary.org/books/OL1413455M/Psychometric_theory.

OECD. (2024). OECD Survey on Drivers of Trust in Public Institutions – 2024 Results: Building Trust in a Complex Policy Environment. OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/07/oecd-survey-on-drivers-of-trust-in-public-institutions-2024-results_eeb36452/9a20554b-en.pdf

Ohemeng, F. L. K., & Ofosu-Adarkwa, K. (2014). Overcoming the digital divide in developing countries: An examination of Ghana’s strategies to promote universal access to information communication technologies (ICTs). Journal of Developing Societies, 30(3), 297-322.

Ølnes, J. (1994). Development of security policies. Computers & Security, 13(8), 628-636.

Ording, L. G., Gao, S., & Chen, W. (2022). The influence of inputs in the information security policy development: an institutional perspective. Transforming Government: People, Process and Policy, 16(4), 418-435.

Orlowski, A. (2018, January 19). OnePlus admits: Up to 40,000 customers' credit card details stolen. The Register. Retrieved from https://www.theregister.com/2018/01/19/oneplus_credit_card_hack/

O'Cathain, A., Murphy, E., & Nicholl, J. (2010). Three techniques for integrating data in mixed methods studies. BMJ, 341, c4587.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behaviour towards IS security policy compliance. Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07), 156b-156b. https://doi.org/10.1109/HICSS.2007.206

Palmer, M. E., Robinson, C., Patilla, J. C., & Moser, E. P. (2001). Information security policy framework: Best practices for security policy in the e-commerce age. Information Systems Security, 10(2), 1-15.

Pathari, V., & Sonar, R. (2012). Identifying linkages between statements in information security policy, procedures and controls. Information Management & Computer Security, 20(4), 264-280.

Patton, M. Q. (2002). Qualitative research and evaluation methods (3rd ed.). SAGE Publications.

Peltier, T. R. (2005). Information security risk analysis. Auerbach Publications. Retrieved from Taylor & Francis: https://www.taylorfrancis.com/books/mono/10.1201/9781420031195/information-security-risk-analysis-thomas-peltier-thomas-peltier.

Peters, B. Guy. "Introducing the Topic". Governance in a Changing Environment, edited by B. Guy Peters and Donald J. Savoie, Montreal: McGill-Queen's University Press, 1995, pp. 3-19. https://doi.org/10.1515/9780773565500-003.

Peterson, R. A. (1994). A meta-analysis of Cronbach's coefficient alpha. Journal of Consumer Research, 21(2), 381-391.

Pett, M. A. (1997). Nonparametric statistics for health care research: Statistics for small samples and unusual distributions (pp. 1-307). Thousand Oaks, CA: SAGE Publications.

Pfleeger, C. P., & Cooper, D. M. (1997). Security and privacy: Promising advances. IEEE Software, 14(5), 27-32.

Pickard, A. J. Research methods in information. London: Facet Publishing, 2013, pp. 1-384.

Pohle, J., & Thiel, T. (2021). Digital sovereignty. In B. Herlo, D. Irrgang, G. Joost, & A. Unteidig (Eds.), Practicing sovereignty: Digital involvement in times of crises (pp. 47-67). Bielefeld: transcript Verlag. Retrieved from https://www.ssoar.info/ssoar/bitstream/handle/document/76237/ssoar-2021-pohle_et_al-Digital_Sovereignty.pdf?sequence=1.

Police and Border Guard Board. (2022). Certificate Policy for identity card, digital identity card, residence permit card and diplomatic identity card (Version 1.1). Retrieved from https://www.id.ee/wp-content/uploads/2022/02/cp_esteid_v1.1.pdf

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. MIS Quarterly, 34(4), 757-778. https://doi.org/10.2307/257507041

PwC. (2014). Global state of information security survey. PricewaterhouseCoopers. Retrieved from https://www.pwc.com/na/en/assets/pdf/global-state-of-information-security-survey-2014-key-findings-report.pdf.

PwC. (2015). 2015 information security breaches survey. Retrieved from https://www.pwc.co.uk/annualreport/assets/2015/PwC-Annual-Report-2015-Financial-Statements.pdf

PricewaterhouseCoopers. (2016). The global state of information security survey 2016. PwC. Retrieved from https://www.pwc.com/sg/en/publications/assets/pwc-global-state-of-information-security-survey-2016.pdf

Qualtrics. (2017). Qualtrics survey platform. Retrieved from https://www.qualtrics.com/xm-survey-platform/.

Raggad, B. G. (2010). Information security management: Concepts and practice. CRC Press. Retrieved from https://www.taylorfrancis.com/books/mono/10.1201/9781439882634/information-security-management-bel-raggad.

Ransbotham, S., & Mitra, S. (2009). Are markets for vulnerabilities effective? MIS Quarterly, 33(1), 29-57.

Raveesh, S. (2013). Digital Divide – "Haves" and "Have-Nots": A Modern Inequality of 21st Century. European Academic Research, 1(7), 131-145. https://euacademic.org/UploadArticle/131.pdf

Rees, J., Bandyopadhyay, S., & Spafford, E. H. (2003). A policy framework for information security. Communications of the ACM, 46(7), 101-106.

Renaud, K., Warkentin, M., Pogrebna, G., & van der Schyff, K. (2024). VISTA: An inclusive insider threat taxonomy, with mitigation strategies. Information & Management, 61(1), 103877.

Richards, T. J., & Richards, L. (1999). Using NVivo in qualitative research. In N. K. Denzin & Y. S. Lincoln (Eds.), Handbook of qualitative research (2nd ed., pp. 445-462). SAGE Publications.

Robles-Carrillo, M. (2024). Digital identity: an approach to its nature, concept, and functionalities. International Journal of Law and Information Technology, 32(1), eaae019.

Robinson, E., & McMenemy, D. (2020). 'To be understood as to understand': A readability analysis of public library acceptable use policies. Journal of Librarianship and Information Science, 52(3), 713-725.

Robinson, S. L. (1996). Trust and breach of the psychological contract. Administrative Science Quarterly, 574-599.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. Academy of Management Review, 23(3), 393-404.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organisations. Computers & Security, 56, 70-82.

Samonas, S., Dhillon, G., & Almusharraf, A. (2020). Stakeholder perceptions of information security policy: Analysing personal constructs. International Journal of Information Management, 50, 144-154.

SANS Institute. (2014). Information security policy templates. Retrieved from https://www.sans.org/information-security-policy

Sasse, M. A., & Flechais, I. (2005). Usable security: Why do we need it? How do we get it? In L. F. Cranor & S. Garfinkel (Eds.), Security and usability: Designing secure systems that people can use (pp. 13-30). O'Reilly Media. Retrieved from https://discovery.ucl.ac.uk/id/eprint/20345/.

Saxby, S. (2006). Influencing behaviours - moving beyond the individual: ISM user guide. gov.scot.

Scandura, T. A., & Williams, E. A. (2000). Research methodology in management: Current practices, trends, and implications for future research. Academy of Management Journal, 43(6), 1248-1264.

Schneier, B. (2006). Secrets and lies: Digital security in a networked world. John Wiley & Sons.

Schmerken, I. (2015). Morgan Stanley data theft exposes insider threat & need for more restrictions. Retrieved June, 10, 2024.

Schober, P., Boer, C., & Schwarte, L. A. (2018). Correlation coefficients: Appropriate use and interpretation. Anesthesia & Analgesia, 126(5), 1763-1768. https://doi.org/10.1213/ANE.0000000000002864

Schutt, R. K. (2018). Investigating the social world: The process and practice of research (9th ed.). Sage Publications. Retrieved from https://books.google.com/books/about/Investigating_the_Social_World.html?id=zkBKDwAAQBAJ.

Shockley-Zalabak, P., Ellis, K., & Winograd, G. (2000). Organisational trust: What it means, why it matters. Organisation Development Journal, 18(4), 35.

Sieber, S. D. (1973). The integration of fieldwork and survey methods. American Journal of Sociology, 78(6), 1335-1359.

Silverman, D. (2000). Doing qualitative research: A practical handbook. SAGE Publications.

Silverman, D. (2001). Interpreting qualitative data: Methods for analysing talk, text and interaction (2nd ed.). SAGE Publications.

Sims, H. (2001). Public confidence in government, and government service delivery. Ottawa: Canadian Centre for Management Development.

Simon, H. A. (1950). Administrative behaviour. AJN The American Journal of Nursing, 50(2), 46-47.

Siponen, M. (2006a). Information security standards focus on the existence of process, not its content. Communications of the ACM, 49(8), 97-100.

Siponen, M. (2006b). Six design theories for IS security policies and guidelines. Journal of the Association for Information Systems, 7(1), 19.

Siponen, M., & Iivari, J. (2006). Six design theories for IS security policies and guidelines. Journal of the Association for Information Systems, 7(7), 445-472. **Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. Information & Management, 46(5), 267–270.** https://doi.org/10.1016/j.im.2008.12.007

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

Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' adherence to information security policies: An empirical study. In New Approaches for Security, Privacy and Trust in Complex Environments: Proceedings of the IFIP TC-11 22nd International Information Security Conference (SEC 2007) (pp. 133-144). Springer US.

Siponen, M., & Vance, A. (2010). Neutralisation: New insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), 487-502. https://doi.org/10.2307/25750688

Siponen, M., & Vance, A. (2014). Guidelines for improving the contextual relevance of field surveys: The case of information security policy violations. European Journal of Information Systems, 23(3), 289-305.

Solove, D. J. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), 477–560. https://doi.org/10.2307/40041279

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2), 215-225.

Soo Hoo, K. J. (2000). How much is enough? A risk-management approach to computer security. CISAC Working Paper. Retrieved from https://cisac.fsi.stanford.edu/publications/how_much_is_enough__a_riskmanagement_approach_to_computer_security.

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. MIS Quarterly, 503-522.

Special Eurobarometer 359. (2011). Attitudes on data protection and electronic identity in the European Union. European Commission. Retrieved from https://joinup.ec.europa.eu/sites/default/files/document/2014-12/Part%20I%20of%20Special%20Eurobarometer%20359%20-%20Attitudes%20on%20Data%20Protection%20and%20Electronic%20Identity%20in%20the%20European%20Union.pdf

Spero, J. (2018). British Airways data breach: What you need to know. TechCrunch. Retrieved from https://techcrunch.com/2018/09/06/british-airways-data-breach/ (accessed on 09/09/2018)

Spencer, K. A., & Darvizeh, Z. (2015). The mental number line: Evidence from numerical cognition. Journal of Cognitive Psychology, 27(3), 345-356.

Spreitzer, G. M., & Mishra, A. K. (1999). Giving up control without losing control: Trust and its substitutes' effects on managers' involving employees in decision making. Group & Organisation Management, 24(2), 155-187.

Stake, R. E. (1995). The art of case study research. Sage Publications. Retrieved from https://books.google.com/books/about/The_Art_of_Case_Study_Research.html?id=ApGdBx76b9kC.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviours. Computers & Security, 24(2), 124-133.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems (NIST Special Publication 800-30). National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30.pdf.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. MIS Quarterly, 441-469.

Straub Jr, D. W. (1990). Effective IS security: An empirical study. Information Systems Research, 1(3), 255-276.

Talbot, S., & Woodward, A. (2009). Improving an organisation's existing information technology policy to increase security.

Talib, Y. Y. A., & Dhillon, G. (2015). Employee ISP compliance intentions: An empirical test of empowerment. ICIS 2015 Proceedings. Association for Information Systems. https://aisel.aisnet.org/icis2015/proceedings/SecurityIS/13/ accessed on 02/03/2025

Tammpuu, P., & Masso, A. (2019). Transnational digital identity as an instrument for global digital citizenship: The case of Estonia's e-residency. Information Systems Frontiers, 21(3), 621-634. https://doi.org/10.1007/s10796-019-09908-y

Tan, K. L., Chi, C.-H., & Lam, K.-Y. (2023). Survey on digital sovereignty and identity: From digitisation to digitalisation. ACM Computing Surveys, 56(3), 1-36.

Tan, et al. (2023). Data sovereignty and digital sovereignty: Ensuring control and security of personal data. Journal of Information Security and Applications, 58, 102-115.

Tashakkori, A., & Teddlie, C. (2003). Handbook of mixed methods in social & behavioural research. Sage Publications. Retrieved from https://books.google.com/books/about/Handbook_of_Mixed_Methods_in_Social_Beha.html?id=F8BFOM8DCKoC.

Taylor, A. (2013). Information security management principles (2nd ed.). BCS The Chartered Institute for IT.

Taylor, A., Alexander, D., Finch, A., & Sutton, D. (2020). Information security management principles (3rd ed.). BCS, The Chartered Institute for IT.

Taylor, S. J., & Bogdan, R. (1998). Introduction to qualitative research methods: A guidebook and resource (3rd ed.). John Wiley & Sons.

Tesch, R. (1990). Qualitative research: Analysis types and software tools. Falmer Press.

Thibault Landry, A., & Whillans, A. (2019). The power of workplace rewards: Using self-determination theory to understand why reward satisfaction matters for workers around the world. Compensation & Benefits Review, 51(3), 1-26.

Thurstone, L. L., & Chave, E. J. (1929). The measurement of attitude: A psychophysical method and some experiments with a scale for measuring attitude toward the church. University of Chicago Press.

Tomkins, C. (2001). Interdependencies, trust and information in relationships, alliances and networks. Accounting, Organisations and Society, 26(2), 161-191.

Tryfonas, T., Kiountouzis, E., & Poulymenakou, A. (2001). Embedding security practices in contemporary information systems development approaches. Information Management & Computer Security, 9(4), 183-197.

Tyler, T. R. (2003). Trust within organisations. Personnel Review, 32(5), 556-568.

Tzafrir, S. S., & Dolan, S. L. (2004). Trust me: A scale for measuring manager-employee trust. Management Research: Journal of the Iberoamerican Academy of Management, 2(2), 115-132.

Uebersax, J. S. (2006). Likert scales: Dispelling the confusion. Retrieved from john-uebersax.com on 23/07/2023

UK Government. (2025). Security Policy Framework. Retrieved from https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework#personnel-security Accessed on 05/05/2025

Unique Identification Authority of India. (2017). Authentication devices & documents. Retrieved from https://UIDAI.gov.in/en/ecosystem/authentication-devices-documents/archive-authentication-doc.html.

U.S. Government. (1974). Privacy Act of 1974. Retrieved from https://www.justice.gov/opcl/privacy-act-1974. Accessed on 05/05/2025

U.S. Government. (2002). E-Government Act of 2002. Retrieved from https://www.congress.gov/bill/107th-congress/senate-bill/803 Accessed on 05/05/2025

Vance, A., & Siponen, M. (2012). IS security policy violations: A rational choice perspective. Journal of Organisational and End User Computing, 24(1), 21-41.

Van Der Schyff, K., Foster, G., Renaud, K., & Flowerday, S. (2023). Online privacy fatigue: A scoping review and research agenda. Future Internet, 15(5), 164. https://doi.org/10.3390/fi15050164

Van de Walle, S. (2004). Perceptions of administrative performance: The key to trust in government? [Doctoral Thesis, KU Leuven]. KU Leuven. Retrieved from https://soc.kuleuven.be/io/english/research/publication/perceptions-of-administrative-performance-the-key-to-trust-in-government.

Vardi, Y., & Weitz, E. (2004). Misbehavior in organizations: Theory, research, and management. Lawrence Erlbaum Associates. Retrieved from https://www.taylorfrancis.com/books/mono/10.4324/9781410609052/misbehavior-organizations-yoav-vardi-ely-weitz-yoav-vardi-ely-weitz.

Verizon. (2016). 2016 data breach investigations report. Verizon Enterprise Solutions. Retrieved from https://www.verizon.com/business/verizonpartnersolutions/business/resources/reports/DBIR_2016_Report.pdf.

Verizon. (2023). 2023 data breach investigations report. Retrieved from https://www.verizon.com/about/news/2023-data-breach-investigations-report

Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security–what goes where? Information & Computer Security, 26(1), 2-9.

Von Solms, R. (1999). Information security management: Why standards are important. Information Management & Computer Security, 7(1), 50-58.

Von Solms, R., & Von Solms, B. (2004). From policies to culture. Computers & Security, 23(4), 275-279.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. Computers & Security, 23(3), 191-198.

Wall, D. S. (2013). Enemies within: Redefining the insider threat in organisational security policy. Security Journal, 26, 107-124.

Wall, J., Lowry, P. B., & Barlow, J. B. (2015). Organisational violations of externally governed privacy and security rules: Explaining and predicting selective violations under conditions of strain and excess. Journal of the Association for Information Systems, 17(1), 39-76.

Walle, S. V. D., Kampen, J. K., & Bouckaert, G. (2005). Deep impact for high-impact agencies?: Assessing the role of bureaucratic encounters in evaluations of government. Public Performance & Management Review, 28(4), 532-549.

Waly, N., Tassabehji, R., & Kamala, M. (2012). Measures for improving information security management in organisations: The impact of training and awareness programmes. UK

Academy for Information Systems Conference Proceedings. Retrieved from https://aisel.aisnet.org/ukais2012/8/.

Warkentin, M., & Johnston, A. C. (2010). IT security governance and centralised security controls. MIS Quarterly, 34(3), 549-571.

Warman, A. R. (1992). Organisational computer security policy: The reality. European Journal of Information Systems, 1(5), 305-310.

Welsh, E. (2002). Dealing with data: Using NVivo in the qualitative data analysis process. Forum Qualitative Sozialforschung / Forum: Qualitative Social Research, 3(2). https://doi.org/10.17169/fqs-3.2.865

Whitman, M. E. (2008). Chapter 6: Security policy: From design to maintenance. In D. W. Straub, S. Goodman, & R. Baskerville (Eds.), Information security: Policy, processes, and practices (pp. 123-151). ME Sharpe.

Whitman, M. E. (2008). Principles of information security. Cengage Learning.

Whitman, M. E., & Mattord, H. J. (2011). Principles of information security (4th ed.). Cengage Learning. Retrieved from https://books.google.com/books/about/Principles_of_Information_Security.html?id=Hwk1EAAAQBAJ.

Whitman, M. E., Townsend, A. M., & Aalberts, R. J. (2001). Information systems security and the need for policy. In Information security management: Global challenges in the new millennium (pp. 9-18). IGI Global.

Whitman, M. E., & Mattord, H. J. (2018). Principles of information security (6th ed.). Cengage Learning.

Wiant, T. L. (2005). Information security policy’s impact on reporting security incidents. Computers & Security, 24(6), 448-459.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. MIS Quarterly, 1-20.

Willits, F. K., Theodori, G. L., & Luloff, A. E. (2016). Another look at Likert scales. Journal of Rural Social Sciences, 31(3), 126-139.

Wladawsky-Berger, I. (2016). Towards a trusted framework for identity and data sharing.

Wood, C. C. (1995). Writing infosec policies. Computers & Security, 5(14), 418.

Woon, I. M., & Kankanhalli, A. (2003). Measuring factors that influence information security effectiveness in organisations. In Proceedings of the 13th Annual Workshop on Information Technologies and Systems (pp. 12-13).

World Bank. (2019). ID4D Practitioner's Guide: Version 1.0 (October 2019). Retrieved from https://documents.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf.

World Economic Forum. (2018). Identity in a digital world – A new chapter in the social contract. Retrieved from https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf.

Wright, P. M., Dunford, B. B., & Snell, S. A. (2003). Human resources and the resource-based view of the firm. Journal of Management, 27(6), 701-721.

Yin, R. K. (2003). Case study research: Design and methods (3rd ed.). Sage Publications. Retrieved from https://books.google.com/books/about/Case_Study_Research.html?id=BWea_9ZGQMwC.

Yin, R. K. (2013). Validity and generalisation in future case study evaluations. Evaluation, 19(3), 321-332.

Zhang, Y., & Wildemuth, B. M. (2016). Qualitative analysis of content. In B. M. Wildemuth (Ed.), Applications of social research methods to questions in information and library science (2nd ed., pp. 318-329). Libraries Unlimited.

Zorzi, M., Priftis, K., & Umiltà, C. (2002). Neglect impairs explicit processing of the mental number line. Nature Neuroscience, 5(6), 593-596.

Zwitter, A., & Boisse-Despiaux, M. (2020). Blockchain for humanitarian action and development aid. Journal of International Humanitarian Action, 5(1), 16. https://doi.org/10.1186/s41018-018-0044-5

9 Appendix

9.1 Study 1 on Internal Stakeholders Survey (NIA Staff Survey) PIS and Ethics Approval

Information Security Policies and their Impact on Electronic Identity System

Participant Information Sheet

Name of Department: Faculty of Science, Department of Computer and Information Sciences.

Title of the study: The impact of Information Security Policies (ISP) on Electronic Identity Systems

My name is Salim Awudu, a full time Ph.D. research student from the Department of Computer and Information Sciences, University of Strathclyde, Glasgow.

Introduction

My research is focused on the impact of Information Security Policies (ISP) on Electronic Identity Systems.

The Department of Computer and Information Science is part of the University of Strathclyde, UK. The University is a charity body registered in Scotland, located at 16 Richmond Street Glasgow, G1 1XQ United Kingdom.

What is the Purpose of this investigation?

The research seeks to gather data on the involvement of staff in the formulation, expression and implementation of the National Identification Authority Information Security Policy (NIA-ISP).

The overall aim of the study is to understand the formulation of NIA's Information Security Policy (ISP) and how it can be enforced and the challenges encountered during compliance.

Do you have to take part?

No. This study is designed to reach the staff of the NIA as participants. Taking part in this study is voluntary. This means that participants have the right to decide on whether to participate in the study or not.

Again, during the study, a participant can decide to change his/her mind to quit by withdrawing from the study without any issue. In other words, there are no penalties for choosing to withdraw from the study without any reason. Similarly, if new information becomes available that may affect the risks or benefits associated with the study or your willingness to participate in it, you will be notified in order to make a decision on whether or not to participate in the study.

What will you do in the project?

The survey study is designed based on answering questions related to Information Security Policy (ISP). People willing to participate can go either online or fill in the paper-based questionnaire. The online option is through the link provided. Participants are required to answer all questions and are free to contact any of the investigators for additional information or question that is not clear to them. The survey is available for a maximum period of 1 and half month and will end on 14th March 2020 for Junior and Senior Staff.

In the case of Management members, an interview would be conducted.

Why have you been invited to take part?

In general, this study is for the staff of the National Identification Authority (NIA) in Ghana.

What are the potential risks to you in taking part?

In this survey, participants may feel uncomfortable to answering some questions as they involve some personal information. In a situation whereby respondents find any question upsetting, they are free to withdraw from the study without any problem. This can be done by clicking on the "End Study Button" which will take you to the end of the study.

What information is being collected in the project?

This study would record some personal information of participants and this includes, gender, and educational level. As the study is highly anonymous, no part of respondent’s information would be shared with a third party. In addition, we will pseudoanoymise/anonymise the data to protect individual participants. The participants would also be advised on the protection of their identity and how the data could be used.

Who will have access to the information?

All information provided in this survey will be kept strictly confidential during collection, analysis as well as when publishing the result of the survey. It is essential for the participants to be aware that their identity will be kept anonymous and the information they provide in this study will be secured in accordance with the university's policy.

The researcher and the Supervisor are the only people that would have access to the primary data collected from participants.

In addition, some of the data we collect which relates to personal information would not be shared and will be destroyed in accordance with the data sharing agreement; the ethics application; and participant consent forms.

The University of Strathclyde is registered with the Information Commissioner's Office who implements the Data Protection Act 2018.

Where will the information be stored and how long will it be kept for?

All the information gathered from this study will be secured and stored in the university of Strathclyde storage facility (Strathcloud). As this is an ongoing research, all data collected from this study can be stored for a maximum period in accordance with University of Strathclyde policy. This would include uploading the data to University of Strathclyde’s institutional data repository, Pure – for a minimum period of 10 years. However, Data which does not relate to any research findings, and is deemed to be of no value, no interest, and not worth sharing, would be deleted.

What happens next?

To proceed and participate in the study, participants can click on the start button. Any individual that needs additional information about the study can contact either the researcher or chief investigator.

Researcher’s contact details:

Name: Salim Awudu

Address: Office no. LT 1220
Department of Computer and Information Sciences
University of Strathclyde

Email address: salim.awudu@strath.ac.uk

Chief Investigator’s details:

Name:	Dr Sotirios Terzis, PhD, MSc, BSc (Hons), CITP, MBCS, FHEA.
Address:	Department of Computer and Information Sciences University of Strathclyde Livingstone Tower, 26 Richmond Str., G1 1XH, Glasgow, Scotland email: sotirios.terzis@strath.ac.uk phone: +44.141.5483839 fax: +44.141.5484523

Ethics Approval

This research was granted Ethical approval by the Department of Computer & Information Science Ethics Committee of the University of Strathclyde.

If you have any questions/concerns, during or after the research, or wish to contact an independent person to whom any questions maybe directed or further information may be sought from, please contact:

Secretary to the Departmental Ethics Committee

Depart of Computer and Information Sciences

Livingston Tower

Richmond Street

Glasgow

G1 1XH

Email: ethics@cis.strath.ac.uk

9.2 The Studies Consent Form

Name of Department: **Faculty of Science, Department of Computer and Information Sciences.**

Title of Research: "The impact of Information Security Policies (ISP) on Electronic Identity Systems".

Participation Consent

I understand the information provided above. I also understand that I have the right to withdraw from the study without any consequences at any point. However, I do appreciate that due to the anonymous data collection, my data may not be possible to be fully removed. On the basis of this understanding, I consent to participate in this study

Signature: Date:

…………………. ……………………..

9.3 Study 1 on Internal Stakeholders Survey (NIA Staff Survey) Questionnaire

Q1 Please tick your gender

Male (1)

Female (2)

Q2 Please select your age range

20-30 (1)

31-40 (2)

41-50 (3)

51-60 (4)

61 and above (5)

Q3 Please select your department or unit

Human Resources (1)

Administration (2)

Technology and Biometrics (3)

Operations (4)

Finance (5)

Internal Control (6)

Other (7)

Q4 How many years have you been working for NIA?

Less than 1 year (1)

1-2 years (2)

3-6 years (3)

6-9 years (4)

More than 9 years (5)

Q5 What is your highest level of education?

Secondary (1)

University Undergraduate (2)

University Postgraduate (3)

Q6 Please select your operational region

Greater Accra Headquarters (Accra) (1)

Ashanti (Kumasi) (2)

Northern (Tamale) (3)

Bono (Sunyani) (4)

Q7 Please select your type of employment with the NIA

Permanent Staff (1)

Contract Staff (2)

Seconded Staff (3)

Q8 I know the rules and regulations prescribed by the Information Security Policy (ISP) of my organisation

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q9 I understand the rules and regulations prescribed by the ISP of my organisation

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q10 I know my responsibilities as prescribed in the ISP to enhance the Information Systems security of my organisation.

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q11 My organisation educates employees on their computer security responsibilities.

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q12 National Identification Authority (NIA) communicates relevant information security requirements to me

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q13 The information security policy is practical.

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q14 I am informed in a timely manner as to how information security changes will affect me.

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q15 The contents of the information security policy were effectively communicated to me.

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q16 The contents of the information security policy are easy to understand

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q17 My pay raises and/or promotions depend on whether I comply with the requirements of the ISP.

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q18 I will receive personal mention in oral or written assessment reports if I comply with the requirements of the ISP.

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q19 I will be given monetary or non-monetary rewards if I comply with the requirements of the ISP.

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q20 My receiving tangible or intangible rewards are tied to whether I comply with the requirements of the ISP.

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q21 My compliance with the requirements of the ISP would make me feel content.

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q22 My compliance with the requirements of the ISP would make me feel satisfied.

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q23 My compliance with the requirements of the ISP would make me feel accomplished.

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q24 My compliance with the requirements of the ISP would make me feel fulfilled.

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q25 Failing to lock or log out of workstation constitutes an Information Security Policy violations

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q26 Writing down personal passwords in visible places constitutes an Information Security Policy violation

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q27 Sharing passwords with colleagues or friends constitutes an Information Security Policy violation

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q28 Copying sensitive data to unencrypted USB drives constitutes an Information Security Policy violation

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q29 Revealing confidential information to outsiders constitutes an Information Security Policy violation

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q30 Disabling security configurations constitutes an Information Security Policy violation

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q31 Using laptops carelessly outside of the company constitutes an Information Security Policy violation

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q32 Sending confidential information unencrypted constitutes an Information Security Policy violation

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q33 Creating easy-to guess-passwords constitutes an Information Security Policy violation

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q34 To me, complying with the requirements of the ISP is

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
Unnecessary (1)							
Necessary (2)							

Q35 To me, complying with the requirements of the ISP is

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
Beneficial (1)							
Unbeneficial (2)							

Q36 To me, complying with the requirements of the ISP is

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
Unimportant (1)							

Important (2)							

Q37 To me, complying with the requirements of the ISP is

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
Useless (1)							
Useful (2)							

Q38 The involvement of executive management in the information security policy development is crucial to the approval of the security policies

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q39 Executive management is involved in the development and revision of the information security policy"

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q40 Employees signing off that, they have received and reviewed the ISP, indicates their agreement to be bound by the information security policies of the NIA.

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q41 It is important to consult employees in the development and revision of the information security policy

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q42 The ISP of the NIA is reasonable

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q43 The ISP of the NIA is not readable

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q44 The ISP of the NIA is not easy to understand

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q45 In my organisation, ISP development and revision involves all employees.

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q46 During the development and any revisions of the ISP, employees are consulted to ensure that its provisions are and remain reasonable

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q47 During the development and any revisions of the ISP, its phrasing is tested with employees to ensure that it is and remains easy to read

Strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

Q48 During the development and any revisions of the ISP employees are actively involved in ensuring it is and remains easy to understand

strongly agree (1)

Agree (2)

Somewhat agree (3)

Neither agree nor disagree (4)

Somewhat disagree (5)

Disagree (6)

Strongly disagree (7)

End of Block: Default Question Block

9.4 Ethics Approvals and Introductory Letters for Interview Studies

Information Security Policies and their Impact on Electronic Identity System

9.4.1 Participant Information Sheet

Name of Department: Faculty of Science, Department of Computer and Information Sciences.

Title of the study: The impact of Information Security Policies (ISP) on Electronic Identity Systems

My name is Salim Awudu, a full time Ph.D. research student from the Department of Computer and Information Sciences, University of Strathclyde, Glasgow.

Introduction

My research is focused on the impact of Information Security Policies (ISP) on Electronic Identity Systems.

The Department of Computer and Information Science is part of the University of Strathclyde, UK. The University is a charity body registered in Scotland, located at 16 Richmond Street Glasgow, G1 1XQ United Kingdom.

What is the Purpose of this investigation?

The research seeks to gather data on the involvement of stakeholders in the formulation, expression and implementation of the National Identification Authority Information Security Policy (NIA-ISP).

The overall aim of the study is to understand the formulation of NIA's Information Security Policy (ISP) and how it can be enforced and the challenges encountered during compliance.

Do you have to take part?

No. This study is designed to reach the stakeholders of the NIA as participants. Taking part in this study is voluntary. This means that participants have the right to decide on whether to participate in the study or not.

Again, during the study, a participant can decide to change his/her mind to quit by withdrawing from the study without any issue. In other words, there are no penalties for choosing to withdraw from the study without any reason. Similarly, if new information becomes available that may affect the risks or benefits associated with the study or your willingness to participate in it, you will be notified in order to make a decision on whether or not to participate in the study.

What will you do in the project?

The study is designed based on answering questions related to Information Security Policy (ISP). People willing to participate can are interviewed using a semi-structured interview guide. Participants are required to answer all questions and are free to contact any of the investigators for additional information or questions that are not clear to them.

Why have you been invited to take part?

In general, this study is for the managerial stakeholders of the National Identification Authority (NIA) in Ghana.

What are the potential risks to you in taking part?

In this study, participants may feel uncomfortable to answering some questions as they involve some personal information. In a situation whereby respondents find any question upsetting, they are free to withdraw from the study without any problem. This can be done by informing the researcher and the researcher will end the study.

What information is being collected in the project?

This study would record some personal information of participants and this includes, gender, and educational level. As the study is highly anonymous, no part of respondent's information would be shared with a third party. In addition, we will pseudoanoymise/anonymise the data to protect individual participants. The participants would also be advised on the protection of their identity and how the data could be used.

Who will have access to the information?

All information provided in this study will be kept strictly confidential during collection, analysis as well as when publishing the result of the survey. It is essential for the participants to be aware that their identity will be kept anonymous and the information they provide in this study will be secured in accordance with the university's policy.

The researcher and the Supervisor are the only people that would have access to the primary data collected from participants.

In addition, some of the data we collect which relates to personal information would not be shared and will be destroyed in accordance with the data sharing agreement; the ethics application; and participant consent forms.

The University of Strathclyde is registered with the Information Commissioner's Office who implements the Data Protection Act 2018.

Where will the information be stored and how long will it be kept for?

All the information gathered from this study will be secured and stored in the university of Strathclyde storage facility (Strathcloud). As this is an ongoing research, all data collected from this study can be stored for a maximum period in accordance with University of Strathclyde policy. This would include uploading the data to University of Strathclyde's institutional data repository, Pure – for a minimum period of 10 years. However, Data which does not relate to any research findings, and is deemed to be of no value, no interest, and not worth sharing, would be deleted.

What happens next?

To proceed and participate in the study, participants can click on the start button. Any individual that needs additional information about the study can contact either the researcher or chief investigator.

Researcher's contact details:

Name:	Salim Awudu
Address:	Office no. LT 1220 Department of Computer and Information Sciences University of Strathclyde
Email address:	salim.awudu@strath.ac.uk

Chief Investigator's details:

Name:	Dr Sotirios Terzis,

PhD, MSc, BSc (Hons), CITP, MBCS, FHEA.

Address: Department of Computer and Information Sciences
University of Strathclyde
Livingstone Tower, 26 Richmond Str., G1 1XH, Glasgow, Scotland
email: sotirios.terzis@strath.ac.uk
phone: +44.141.5483839
fax: +44.141.5484523

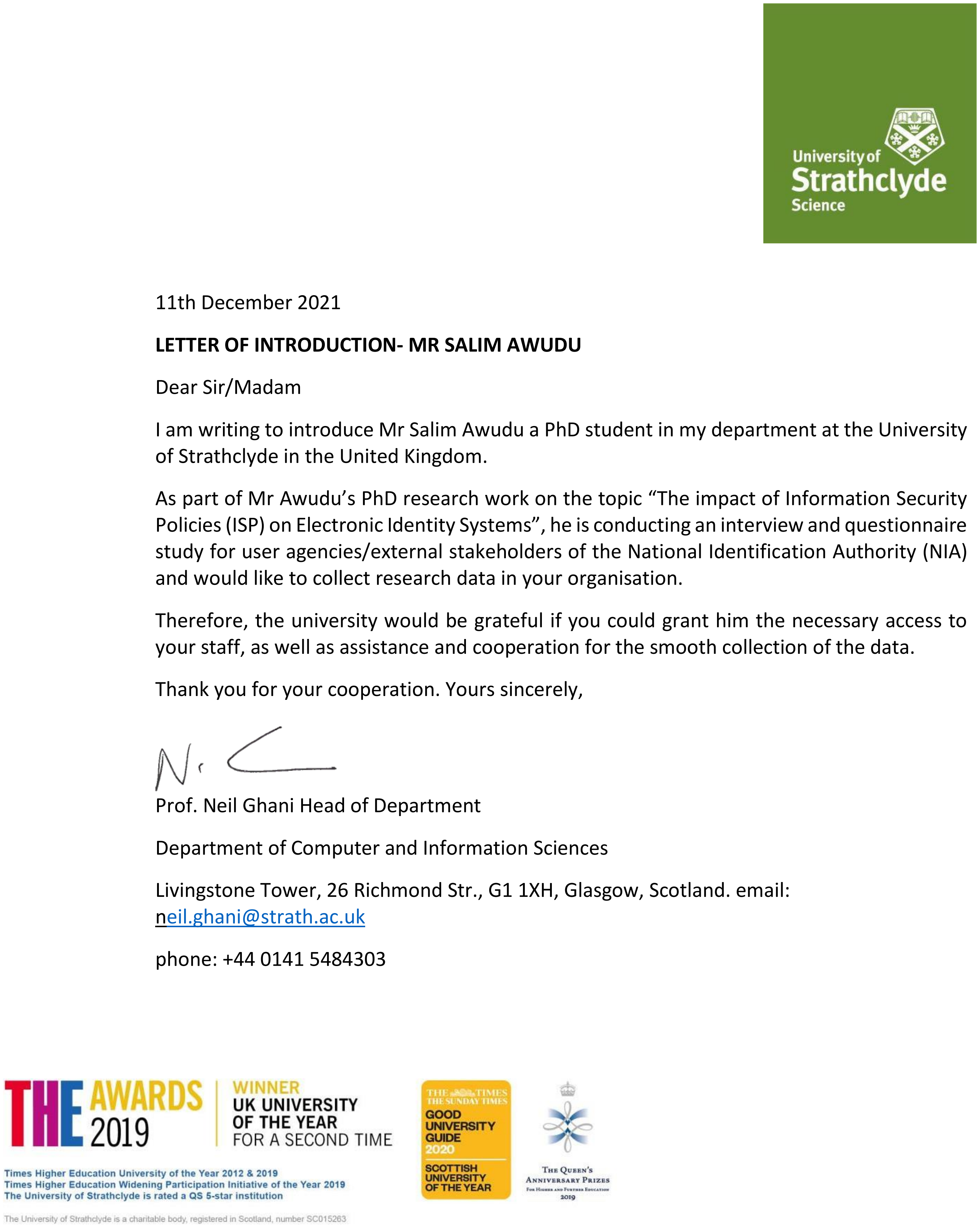
Ethics Approval

This research was granted Ethical approval by the Department of Computer & Information Science Ethics Committee of the University of Strathclyde.

If you have any questions/concerns, during or after the research, or wish to contact an independent person to whom any questions maybe directed or further information may be sought from, please contact:

Secretary to the Departmental Ethics Committee
Depart of Computer and Information Sciences
Livingston Tower
Richmond Street
Glasgow
G1 1XH
Email: ethics@cis.strath.ac.uk

9.4.2 Letter of Introduction from CIS Head



University of Strathclyde
Science

11th December 2021

LETTER OF INTRODUCTION- MR SALIM AWUDU

Dear Sir/Madam

I am writing to introduce Mr Salim Awudu a PhD student in my department at the University of Strathclyde in the United Kingdom.

As part of Mr Awudu’s PhD research work on the topic “The impact of Information Security Policies (ISP) on Electronic Identity Systems”, he is conducting an interview and questionnaire study for user agencies/external stakeholders of the National Identification Authority (NIA) and would like to collect research data in your organisation.

Therefore, the university would be grateful if you could grant him the necessary access to your staff, as well as assistance and cooperation for the smooth collection of the data.

Thank you for your cooperation. Yours sincerely,

Prof. Neil Ghani Head of Department

Department of Computer and Information Sciences

Livingstone Tower, 26 Richmond Str., G1 1XH, Glasgow, Scotland. email: neil.ghani@strath.ac.uk

phone: +44 0141 5484303

THE AWARDS 2019 WINNER UK UNIVERSITY OF THE YEAR FOR A SECOND TIME

Times Higher Education University of the Year 2012 & 2019
Times Higher Education Widening Participation Initiative of the Year 2019
The University of Strathclyde is rated a QS 5-star institution

THE TIMES THE SUNDAY TIMES GOOD UNIVERSITY GUIDE 2020 SCOTTISH UNIVERSITY OF THE YEAR

The Queen's Anniversary Prizes For Higher and Further Education 2019

The University of Strathclyde is a charitable body, registered in Scotland, number SC015263

9.4.3 Letter of Introduction from Supervisor

University of Strathclyde Science

11th December 2021

LETTER OF INTRODUCTION- MR SALIM AWUDU

Dear Sir/Madam

I am writing to introduce Mr Salim Awudu a PhD student at the Department of Computer and Information Sciences, University of Strathclyde, United Kingdom.

Mr Awudu is undertaking a PhD on “The impact of Information Security Policies (ISP) on Electronic Identity Systems” under my supervision. As part of his research work, he is conducting an interview and questionnaire study for user agencies/external stakeholders of the National Identification Authority (NIA) and would like to collect research data in your organisation.

The aim of the research is to determine:

The awareness and understanding by NIA user agencies/external stakeholders of the provisions of the NIA ISP.

Their expectations/perceptions/feelings about the contents and provisions of the NIA ISP.

Their beliefs regarding compliance to the provisions of the NIA ISP.

Their involvement/influence in the development of the NIA ISP.

I would, therefore, be grateful if you could grant him the necessary access to your staff, as well as assistance and cooperation for the smooth collection of the data.

Thank you for your cooperation.

Yours sincerely,

Dr Sotirios Terzis, PhD, MSc, BSc (Hons), CITP, MBCS, FHEA. Lecturer

Department of Computer and Information Sciences

Livingstone Tower, 26 Richmond Str., G1 1XH, Glasgow, Scotland

email: sotirios.terzis@strath.ac.uk, phone: +44.141.5483839, fax: +44.141.5484523

Appendix 8: Semi-Structured Interview Guide for Internal Stakeholders- Management

9.5 Semi-Structured Interview Guide for Study 2 on NIA Management Views

1. Personal Information

What is/was your position in the NIA?

How long have you been/were on that position?

What are/were your main responsibilities?

Have you served the NIA in any other positions? If yes, what kind of positions and for how long?

2. Personal views and thoughts on Information Security and its Management

In your view how much of a concern is Information Security for the NIA? Why?

Do you believe that this is appropriate?

Where does responsibility for managing IS in NIA lay?

What is the role of senior NIA management in ensuring information is secured?

How effective do you think ISM in NIA is?

3. Information Security Policy

Does the NIA have an Information Security Policy?

What do you think are the reasons that the NIA ISP has not been finalised yet?

a. Relevance

How important do you believe it is for the NIA to have an ISP? Why?

b. Content

What are/do you expect to be the key provisions of the NIA ISP?

How good do you think the NIA ISP is/What would make an NIA ISP good? Why?

c. Development

What was/do you expect to be the process for the development of the NIA ISP?

What was/do you expect to be the role of senior management in the development of the NIA ISP?

Who was/do you expect to be involved in the development of the NIA ISP?

What were/do you expect to be the main challenges in the development of the NIA ISP?

How were these challenges addressed/do you expect to address these challenges?

d. Evolution

What is/do you expect to be the process for the evolution (i.e. making amendments) of the NIA ISP?

What is/do you expect to be the role of senior management in the ISP evolution process?

Who is/do you expect to be involved in the ISP evolution process?

How effective do you believe the NIA ISP governance process is?

e. Awareness

What are/do you expect to be the mechanisms used to make staff aware of the provisions of the NIA ISP?

What is/do you expect to be the role of senior management in ensuring that staff are aware of the provisions of the NIA ISP?

How aware do you believe that staff are of the provisions of the NIA ISP?

What are/do you expect to be the main challenges in ensuring staff ISP awareness?

How are these challenges addressed/do you expect to address these challenges?

f. Enforcement

To what extent do you believe that NIA staff do comply with the provisions of the ISP?

How is/do you expect to be staff compliance to the NIA ISP enforced? Are there particular sanctions and/or rewards in place/What would you expect to be the sanctions and/or rewards for non-compliance/compliance to the ISP?

How aware do you believe that staff are of these sanctions/rewards?

How is/would you expect to be compliance to the ISP monitored?

What is/would you expect to be the role of senior management in ISP compliance monitored?

How effective do you believe the NIA ISP is in protecting the security of information?

Do you have any suggestions on how its effectiveness could be improved?

Procedural issues

When approaching participants for an interview, the researcher was clear with them about what the interview would cover and told them that their participation was voluntary and they were free to not answer any questions they were not comfortable with, or even to withdraw from the interview at any point. The researcher also explained to them how the interview transcripts would be managed (i.e. what the research data management plan specified).

9.6 Semi-Structured Interview Guide for External Stakeholders View (User Agencies)

1. Personal Information

What is your position in your organisation?

How long have you been/were on that position?

What are/were your main responsibilities in your organisation?

What is the relationship between your organisation and the NIA?

Is the relationship formalised (e.g. law, regulatory framework, etc)?

For what functions does your organisation rely on the NIA?

Does your organisation have any influence on the operation of the NIA (e.g. formal representation individually or industry wide, advisory body, etc)?

2. Importance and concerns about Information Security and its Management

In your view how much of a concern is Information Security for the NIA? Why?

Do you believe that this is appropriate?

In your view how much of a concern is Information Security to your organisation? Why?

How does the NIS affect the operations of your organisation?

Who is responsibility for managing IS in your organisation?

What is the role of senior management in ensuring information is secured in your organisation?

How effective do you think ISM in your organisation is?

3. Information Security Policy

Based on your understanding of how information security is managed in your organisation would you expect NIA to have an ISP?

How important do you think this is?

What key provisions do you expect the NIA ISP to contain?

Which of them will be essential for the relationship between your organisation and the NIA?

What do you think are the reasons that the NIA ISP has not been finalised yet?

a. Relevance

How important do you believe it is for the NIA to have an ISP? Why?

b. Content

What key provisions of the NIA ISP affect/ do you expect to affect your organisation?

How inputs do you think could be made to the NIA ISP /What would make an NIA ISP good to meet the expectations of your organisation? Why?

c. Development

Would you expect your organisation's concerns to be considered/influence the development of the NIA ISP?

Is there a mechanism for this?

d. Evolution

What is/do you expect to be the process for the evolution (i.e. making amendments) of the NIA ISP?

What is/do you expect to be the role of your organisation in the ISP evolution process?

Who is/do you expect to be involved in the ISP evolution process?

Would you expect your organisation's concerns to be considered/influence the evolution of the NIA ISP?

Is there a mechanism for this?

How effective do you believe the NIA ISP governance process is?

How important is it for your organisation that NIA has an effective ISP governance process?

Do you believe the current process is effective?

Awareness

How do you expect (based on your experience …) NIA should ensure that staff are aware and comply with its ISP?

From your organisation's interaction with NIA staff, do you believe that ISP awareness and compliance monitoring is effective?

Enforcement

To what extent do you believe that your organisation's staff do comply with the relevant provisions of the NIA ISP?

(Note: the above question is only relevant if the answer earlier was that there is an ISP)

How does the NIA ISP impact on the overall mandate/functions of your organisation?

How is/do you expect to be compliance to the relevant NIA provisions ISP enforced?

(note: the above question is only relevant if the answer earlier was that there is an ISP)

Do you believe that the NIA ISP is effective?

Do you believe that the NIA ISP is effective in protecting the information security of your organisation?

Are there any particular areas of concern? What are they?

Are there any areas for improvement?

Procedural issues

When approaching participants for an interview, the researcher was clear with them about what the interview would cover and told them that their participation was voluntary and they were free to not answer any questions they were not comfortable with, or even to withdraw from the interview at any point. The researcher also explained to them how the interview transcripts would be managed (i.e. what the research data management plan specified).

9.7 Study 4 on General Public Survey PIS and Ethics Approval

Information Security Policies and their Impact on Electronic Identity System

Participant Information Sheet

Name of Department: Faculty of Science, Department of Computer and Information Sciences.

Title of the study: The impact of Information Security Policies (ISP) on Electronic Identity Systems

My name is Salim Awudu, a full time Ph.D. research student from the Department of Computer and Information Sciences, University of Strathclyde, Glasgow.

Introduction

My research is focused on the impact of Information Security Policies (ISP) on Electronic Identity Systems.

The Department of Computer and Information Science is part of the University of Strathclyde, UK. The University is a charity body registered in Scotland, located at 16 Richmond Street Glasgow, G1 1XQ United Kingdom.

What is the Purpose of this investigation?

The research seeks to gather data on the perception and views of the public about the formulation, expression and implementation of the National Identification Authority Information Security Policy (NIA-ISP).

The overall aim of this study is to understand the perception, expectations and public beliefs about trust for the NIA and trust for NIA employees, how it can be enforced and the challenges encountered during implementation and compliance.

Do you have to take part?

No. This study is designed to reach the public who are users and the beneficiaries of the NIA services as participants. Taking part in this study is voluntary. This means that participants have the right to decide on whether to participate in the study or not.

Again, during the study, a participant can decide to change his/her mind to quit by withdrawing from the study without any issue. In other words, there are no penalties for choosing to withdraw from the study without any reason. Similarly, if new information becomes available that may affect the risks or benefits associated with the study or your willingness to participate in it, you will be notified in order to make a decision on whether or not to participate in the study.

What will you do in the project?

The survey study is designed based on answering questions related to Information Security Policy (ISP). People willing to participate can go either online or fill in the paper-based questionnaire. The online option is through the link provided. Participants are required to answer all questions and are free to contact any of the investigators for additional information or question that is not clear to them. The survey is available for a maximum period of 1 and half month and will end on 23rd January, 2021 for the General Public.

In the case of Management members of the other external stakeholders, an interview would be conducted.

Why have you been invited to take part?

In general, this study is for members of the public who use or benefit from the services of the National Identification Authority (NIA) in Ghana.

What are the potential risks to you in taking part?

In this survey, participants may feel uncomfortable to answering some questions as they involve some personal information. In a situation whereby respondents find any question upsetting, they are free to withdraw from the study without any problem. This can be done by clicking on the "End Study Button" which will take you to the end of the study.

What information is being collected in the project?

This study would record some personal information of participants, and this includes, gender, and educational level. As the study is highly anonymous, no part of respondent's information would be shared with a third party. In addition, we will pseudoanoymise/anonymise the data to protect individual participants. The participants would also be advised on the protection of their identity and how the data could be used.

Who will have access to the information?

All information provided in this survey will be kept strictly confidential during collection, analysis as well as when publishing the result of the survey. It is essential for the participants to be aware that their identity will be kept anonymous and the information they provide in this study will be secured in accordance with the university's policy.

The researcher and the Supervisor are the only people that would have access to the primary data collected from participants.

In addition, some of the data we collect which relates to personal information would not be shared and will be destroyed in accordance with the data sharing agreement; the ethics application; and participant consent forms.

The University of Strathclyde is registered with the Information Commissioner's Office who implements the Data Protection Act 2018.

Where will the information be stored and how long will it be kept for?

All the information gathered from this study will be secured and stored in the university of Strathclyde storage facility (OneDrive). As this is ongoing research, all data collected from this study can be stored for a maximum period in accordance with University of Strathclyde policy. This would include uploading the data to University of Strathclyde's institutional data repository, Pure – for a minimum period of 10 years. However, Data which does not relate to any research findings, and is deemed to be of no value, no interest, and not worth sharing, would be deleted.

What happens next?

To proceed and participate in the study, participants can click on the start button. Any individual that needs additional information about the study can contact either the researcher or chief investigator.

Researcher's contact details:

Name: Salim Awudu

Address: Office no. LT 1220
Department of Computer and Information Sciences
University of Strathclyde

Email address: salim.awudu@strath.ac.uk

Chief Investigator's details:

Name: Dr Sotirios Terzis,
PhD, MSc, BSc (Hons), CITP, MBCS, FHEA.

Address: Department of Computer and Information Sciences
University of Strathclyde
Livingstone Tower, 26 Richmond Str., G1 1XH, Glasgow, Scotland
email: sotirios.terzis@strath.ac.uk
phone: +44.141.5483839
fax: +44.141.5484523

Ethics Approval

This research was granted Ethical approval by the Department of Computer & Information Science Ethics Committee of the University of Strathclyde.

If you have any questions/concerns, during or after the research, or wish to contact an independent person to whom any questions maybe directed or further information may be sought from, please contact:

Secretary to the Departmental Ethics Committee
Depart of Computer and Information Sciences
Livingston Tower
Richmond Street
Glasgow
G1 1XH
Email: ethics@cis.strath.ac.uk

9.8 Study 4 on General Public Survey Questionnaire

Q1 Please tick your gender

□ Male (1)

□ Female (2)

Q2 Please select your age range

o 20-30 (1)

o 31-40 (2)

o 41-50 (3)

o 51-60 (4)

o 61 and above (5)

Q3 What is your highest level of education?

o Secondary (1)

o University Undergraduate (2)

o University Postgraduate (3)

Q4 It is important that the NIA explains to the public for which purposes their personal information will be used.

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q5 It is important that the NIA explains to the public how their personal information will be secured.

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q6 It is important that the NIA explains to the public how their personal information is secured when shared with other organisations (government organisations, banks, telecoms).

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q7 It is important that the public is involved in the development of the NIA ISP.

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q8 It is important that the public is consulted for any amendments of the NIA ISP.

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q9 It is important that the NIA ensures its staff are aware of the provisions of its ISP

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q10 It is important that the NIA ensures its staff comply with the provisions of its ISP

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q11 The NIA has explained to the public for which purposes their personal information will be used

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q12 The NIA has explained to the public how it ensures that their personal information cannot be accessed by unauthorized parties

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q13 The NIA has explained to the public how it ensures that their personal information cannot be modified by unauthorised parties.

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q14 The NIA has explained to the public how it ensures that their personal information is available for authorised parties to use.

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q15 The NIA has explained to the public how it ensures that their personal information is protected when shared with other organisations (government organisations, banks, telecoms).

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q16 The NIA informs the public in a timely manner as to how information security changes will affect the security of their personal information

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q17 The NIA is effective in protecting citizen personal information

o strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q18 The NIA is skillful in protecting citizen personal information.

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q19 The NIA is very knowledgeable about information security.

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q20 The NIA performs its role of protecting citizen personal information very well.

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q21 If citizens need help in protecting their personal information, the NIA will do its best to help them.

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q22 I believe the NIA acts in the best interest of citizens when managing their personal information.

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q23 The NIA is interested in the wellbeing of citizens when managing their personal information.

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q24 The NIA is truthful in its dealings with citizens about the handling of their personal information.

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q25. The NIA is sincere with citizens about the handling of their personal information.

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q26. The NIA keeps its commitments to protect citizen personal information

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q27. The NIA is honest about the handling of citizen personal information.

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q28. The NIA has involved the public in the development of its ISP.

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q29. The NIA consults the public for any amendments to its ISP.

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q30. NIA employees are effective in protecting my personal information

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q31. NIA employees are skillful in protecting my personal information.

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q32. NIA employees are very knowledgeable about information security.

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q33. NIA employees perform their role of protecting my personal information very well.

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q34. If I need help in protecting my personal information, NIA employees will do their best to help me

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q35. I believe NIA employees act in my best interest when managing my personal information.

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q36. NIA employees are interested in my wellbeing when managing my personal information

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q37. NIA employees are truthful in their dealings with me about the handling of my personal information

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q38. NIA employees are sincere with me about the handling of my personal information.

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

o Disagree (6)

o Strongly disagree (7)

Q39. NIA employees keep their commitments to protect my personal information.

o Strongly agree (1)

o Agree (2)

o Somewhat agree (3)

o Neither agree nor disagree (4)

o Somewhat disagree (5)

- Disagree (6)
- Strongly disagree (7)

Q40. NIA employees are honest about the handling of my personal information

- Strongly agree (1)
- Agree (2)
- Somewhat agree (3)
- Neither agree nor disagree (4)
- Somewhat disagree (5)
- Disagree (6)
- Strongly disagree (7)

End of Block: Default Question Block

9.9 Study 2 on NIA Management Views and Study on External Stakeholders Views (User Agencies) Transcripts

Additional information about the interviews transcriptions (Management Study and User Agencies Study) can be accessed at the link below: https://strath-my.sharepoint.com/:f:/r/personal/salim_awudu_strath_ac_uk/Documents/Desktop/4th%20Year/PhD%20External?csf=1&web=1&e=YyLbZY.

9.10 Study 4 on General Public Survey Gender Analysis

Additional information about the Gender Analysis on the Public survey data can be accessed at the link below: https://strath-my.sharepoint.com/:f:/r/personal/salim_awudu_strath_ac_uk/Documents/Desktop/4th%20Year/PhD%20External?csf=1&web=1&e=YyLbZY.