ADDIS ABABA UNIVERSITY

ADDIS ABABA INSTITUTE OF TECHNOLOGY - AAiT

SCHOOL OF INFORMATION TECHNOLOGY AND ENGINEERING - SiTE

Cybersecurity Governance Framework for Ethiopian National Identification Program

By

Selwa Nurye Hussen

Advisor: Henock Mulugeta (Ph.D)

June 2025

Addis Ababa, Ethiopia

Approval

This is to certify that the thesis prepared by Selwa Nurye Hussen, entitled *"Cybersecurity Governance Framework for the Ethiopian National Identification Program"*, submitted in partial fulfillment of the requirements for the Degree of Master of Science in Cybersecurity (Cybersecurity Governance and Management), complies with the regulations and guidelines of the university and meets the accepted standards of originality and quality.

Signed by the Examining Committee(SGC):

	Name	**Signature**	**Date**
1.	Adviser: Henock Mulugeta, PhD	_____	_____
2.	Coordinator: Sileshi Demesie, PhD	_____	_____
3.	Internal Eximiner: Elefelious Getachew, PhD	_____	_____
4.	External Examiner: Fitsum Assamnew, PhD	_____	_____

Aknowledgment

All praise and thanks are due to Allah, the Most Gracious, and the Most Merciful, for granting me the strength, health, and perseverance to complete this thesis. His guidance has been my source of clarity and resilience throughout this journey.

I would like to express my deepest gratitude to my advisor, Dr. Henock Mulugeta for his consistent support, expert guidance, and constructive feedback throughout the course of this research. His mentorship has been invaluable in shaping both the process and outcome of this work.

I would like to extend my profound gratitude to my family and close friends for their unwavering patience, encouragement, and emotional support throughout this journey. Their belief in me has been a constant source of motivation.

I wish to express my heartfelt appreciation to all the individuals who participated in the data collection phase of this study, particularly those from the Ethiopian National ID Program (ENIDP). The generous contribution of time, insights, and experiences was vital to the depth and credibility of this research. Such openness and cooperation provided a solid foundation for meaningful analysis, and I am truly grateful for the trust and engagement shown throughout the process.

Lastly, I am also thankful to my colleagues and peers at the university for their encouragement, helpful discussions, and collaboration, which contributed to a productive academic environment.

To all who supported this work in any way, please accept my sincere appreciation.

Abstract

Ethiopia launched its digital transformation strategy, Digital Ethiopia 2025, in 2020 to build a sustainable digital economy. One of the key priorities of this strategy is to implement digital identification for all citizens and residents. Digitalizing government services and businesses requires a secure, electronic representation of individuals and entities, proving their identity and reliability during transactions or interactions, both online and in person. However, the increasing interconnectivity of the digital world poses ongoing cybersecurity challenges. Digital IDs, while crucial to enabling the digital economy, are vulnerable to the same cyber risks that affect other widely used digital technologies. Although global efforts to develop national digital identity systems aim to enhance security and convenience, they also face significant technical, ethical, and security challenges. These systems are vital for achieving the Sustainable Development Goals (SDGs), but they often grapple with issues such as privacy, data management, enrollment processes, and costs. As a result, effective cybersecurity governance is essential. The cybersecurity governance activities of the body responsible for overseeing these programs must align closely with the strategy's objectives.

This study employed a qualitative research methodology, including in-depth interviews and document analysis, to collect the necessary data. Thematic data analysis was used to process the data, leading to conclusions from which recommendations were derived. Based on the findings and insights from reviewed literatures, we developed a cybersecurity governance framework that was validated through hypothetical cyber incident scenarios to show that the proposed framework mitigate those incidents. Besides, key performance indicators were prepared to assess the effectiveness of the framework in real-world scenarios.

Keywords*:* **Digital Identity, National Digital Identity, Cybersecurity, Cybersecurity Governance Framework**

Contents

List of Figures

List of Tables

Acronyms and/or Abbreviations and Definitions

ABIS	Automated Biometric Identification System
APTs	Advanced Persistent Threats
ENIDP	Ethiopian National Identification Program
IBM SPSS	IBM Statistical Package for the Social Sciences
IDMS	ID Management system
ID4D	Identification for Development
INS	Immigration and Nationality Service
INVEA	Immigration, Nationality, and Vital Events Agency
INSA	Information Network Security Administration
ICT	Information Communication Technology
IT	Information Technology
KYC	Know Your Customer
MInT	Ministry of Innovation and Technology
MOP	Ministry of Peace
MOSIP	Modular Open Source Identity Platform
NID	National Identification
NIDP	National Identification Program
NIDPE	National Identification Program Ethiopia
NISS	National Intelligence and Security Service
PMO	Prime Minister Office
SSN	Social Security Number

Chapter One: Introduction

1. Introduction

The history of identification dates back thousands of years. The first mention of a government collecting the personal information of its citizens dates to 3800 BC, during the Babylonian Empire (veriff, 2022). Since then, the way we have proven our identity has changed massively. Initially, just pieces of paper, today's identification documents contain several security features that make them incredibly difficult to forge. As time progressed, the way data was collected improved. Fast forward to the Roman Empire, and personalized information was collected for the first time. As a result, a variety of documents were introduced. These included birth certificates, land title deeds, and citizenship records. However, although many of these documents are still issued today, the earliest example of what could be deemed ‘modern ID’ can be traced back to 1414. At this time, King Henry V of England was issued the first-ever passport (Ibid). Issued so citizens could prove their identity while abroad, these papers were then referred to as ‘safe conduct’ documents.

In 1829, the British Parliament enacted the reforms of Robert Peel to place more emphasis on printed police records (Trulioo, 2019). Due to this new focus, data could be stored in a personal document file and linked back to individuals using a unique numerical value. This would be the precursor to more modern government databases that link to ID cards. Building on Robert Peel’s reforms, the Netherlands started its own decentralized Personal Number (PN) system in 1849, but only moved on to issue personal ID cards to each citizen in 1940 (Ibid). By this time, the United States had also begun rolling out its Social Security number cards, the first batch distributed in

1936. Other countries followed suit as electronic data processing continued to permeate countries and governments around the world.

Throughout history, various methods have been used to verify identity, from jewelry as personal markers 100,000 years ago to tattoos marking prisoners in ancient China (Thales, 2022). Passports originated under King Henry V, and personal identification numbers emerged in 1829 with British police records. The first practical use of fingerprints as identifiers began in 1858, followed by the introduction of passwords in ancient Rome and modern computers. In the 2000s, biometric technology surged with palm print databases and India's Aadhaar system, leading to today's widespread use of fingerprint and facial recognition. Technological breakthroughs revolutionized identity verification. In 1840, photography was used for identification, followed by Sir William Herschel's introduction of fingerprints in 1858 (ibid). Digitization began in 1977, with the U.S. linking paper records across institutions, leading to smart identity cards in the late 1980s in countries like Germany and Spain. Biometric advances included automated palm print databases in 2004 and India's Aadhaar system in 2010. Today, e-commerce growth has made identity verification, through Know Your Customer (KYC) and Anti-Money Laundering (AML) policies, critical in combating fraud and money laundering.

The evolution of national ID cards has been shaped by historical events and political needs. Starting with Napoleonic reforms in 19th-century France, national ID systems expanded globally, particularly during World War II (Jerzak, 2015). Countries adopted these systems to consolidate state institutions and manage crises. Post-WWII, Asia saw rapid adoption as governments asserted authority, and later, events like 9/11 and European unification further accelerated their use. Modern ID cards increasingly incorporate biometrics, often introduced following political or economic shocks to strengthen security and governance.

National ID cards are valuable for addressing illegal work, crime, and enhancing public services, but they also present challenges like identity theft risks, privacy concerns, high administrative costs, and increased surveillance (Alkhurayyif, May 2013). A major concern is their dependence across industries, making cyber-attacks or system failures potentially disruptive to an entire economy. National digital identity systems are essential for modernizing public services and enhancing efficiency by accurately identifying individuals and streamlining access to services. These systems offer significant advantages, including increased convenience, reduced costs, and

enhanced security and privacy for users, while also providing the private sector with opportunities for higher revenue and reduced service delivery costs. However, they present challenges such as managing complex cybersecurity risks, the potential for centralized data storage vulnerabilities, and the irreversible nature of biometric data leaks. Additionally, there are concerns about mass surveillance and exclusion risks that need to be addressed through comprehensive legal frameworks and robust governance. Effective implementation requires careful balancing of benefits with privacy and security considerations to ensure that these systems serve their intended purpose without compromising individual rights (Biji Scaria, 2022).

This thesis is initiated to investigate the Ethiopian National Identification Document Program (ENIDP), focusing on cybersecurity implications, and to propose a comprehensive cybersecurity governance framework. The objective was to explore how the program could harness the benefits of enhanced identification and service delivery while addressing potential cybersecurity challenges. By developing a tailored governance framework, the thesis aimed to ensure that the program not only maximized its advantages but also effectively mitigated risks such as data breaches, privacy violations, and system vulnerabilities, thereby supporting the secure and efficient implementation of Ethiopia's digital identity initiative.

1.1. Background of the Study

The ENIDP has gone through different stages which are classified into four chronological periods. The stages are named the initiation, the pre-project preparation, the technical and legal platform development, and the starting (ENIDP, 2023).

The first stage is the initiation of the idea of the ENIDP which was in 2011. The idea of the National ID program was initially considered by the government of Ethiopia back in 2011. It was initiated under the National Intelligence and Security Service (NISS) in cooperation with the Information Network Security Administration (INSA) and other government bodies having oversight over its status. Furthermore, until early 2018, the former INVEA (currently named INS – Immigration and Nationality Service) had been coordinating the effort of establishing a digital ID platform. However, due to many challenges, previous efforts did not progress as expected and produced practical results. During this period, several discussions were conducted on its advantages and

importance for the sustainable development of a country and the conceptual groundwork for the current fast and pragmatic progress and potential.

The second stage occurred in 2018. The Prime Minister's Office (PMO) re-initiated the program with the Ministry of Peace (MOP) and Ministry of Innovation and Technology (MInT), tasking them with carrying out the operation. Strategic documents had been prepared that gave the program the conceptual ground to define the major directions of the ENIDP.

The third stage was from 2019 to 2021. This was a period when technical and legal platform development was finalized. The program was led by the MOP, in cooperation with the MInT as well as the Prime Minister's Office. At this time draft ID law was prepared, technology platform selection was made, and a laboratory-based, as well as a field-based soft pilot, was launched.

The last stage was the period when the ENIDP launched in a full-fledged manner. This occurred in September 2021. The ENIDP has been restructured to report to the Prime Minister’s Office. This was done considering the inter-sectoral nature of a foundation ID system. The program now aims to deliver digital ID to 95% of the adult population by the end of 2025.

Now, the ENIDP is working to enroll and provide Digital Identification to all residents in Ethiopia to provide advanced financial, social, public, and other services that identify a physical person using foundational individualizing mechanisms rather than functional ones. The ENIDP intends to issue Digital IDs to over 70 million citizens and residents in Ethiopia by the end of 2025. The overall registration process has a series of procedures that include, sensitization and awareness creation, collecting individuals' consent to collect information, documentation of identity proof, data collection, and registration validation (Ibid).

1.2. Motivation for the Study

The motivations driving this research are multifaceted. Firstly, the ENIDP is deemed to be the core area upon which the 2025 Ethiopian digital strategy is leveraged. As a result, studying the program and addressing its cybersecurity governance challenges will have a profound impact on the country's digital transformation agenda. Ensuring the security of this program is not only crucial to its own success but also to the broader digitization efforts in Ethiopia. Secondly, as the ENIDP becomes integral to the daily activities of Ethiopian citizens and residents, the security of this

program is paramount. Whether for financial transactions, accessing healthcare, or receiving social services, individuals will depend heavily on the ENIDP. Therefore, addressing the cybersecurity risks associated with the program is vital to ensuring the seamless operation of various sectors across the country. Thirdly, critical national infrastructures such as finance, education, health, and social services will rely on the ENIDP to provide secure, unique identification for their users. The program's core functionalities, including identification, verification, and authentication, will be essential in ensuring the integrity of services across these sectors. These functions will enable users to securely access a wide range of services, verify their identities, and authorize transactions or interactions with various platforms. A successful cyber-attack on this program could compromise these critical processes, acting as a single point of failure, with the potential to cause widespread disruption across multiple sectors. The interdependence of these sectors on a secure identification system makes the ENIDP a prime target for cyber threats, and any vulnerabilities could be exploited to devastating effect. Consequently, proactively curbing such problems by making a study on the program, and pinpointing its problems before it is too late is crucial.

1.3. Statement of the Problem

In the cybersecurity era, digital identity management faces challenges such as privacy concerns, identity theft, data breaches, and regulatory complexities, highlighting the need for enhanced protective measures, ethical data use, and robust frameworks (Ghadge, 2024). Adopting advanced technologies like machine learning, blockchain, and encryption, alongside stronger data protection regulations, is crucial for securing digital identities. Digital ID systems also streamline identification, reduce fraud risks, and improve access to services like banking and healthcare, promoting a more efficient and inclusive society. Countries like Estonia, India, and Singapore, as well as the EU's eIDAS 2.0, exemplify these advancements in digital identity systems (Hendrickson, 2024). These studies discussed digital identity management and digital ID systems in general focusing on their shortcomings and their advantages. Yet, they failed to study the topics under consideration in light of cybersecurity governance paying particular attention to strategic alignment with general objectives, leadership oversight, proper resource allocation, and legal and regulatory enforcement and accountability. Especially, they are not focusing on developing a particular cybersecurity governance framework for the national ID programs.

As national identification programs are based upon biometrics and smart-card-related technologies, they can provide benefits like improved security against identity theft and fraud, as well as increased convenience in various transactions (Smith, 2008). However, national digital identification systems are not devoid of concerns. These concerns are related to technical, ethical, and security aspects requiring robust data protection measures to prevent misuse by hackers or governments (Chan, 2015). The World Bank's ID4D initiative aims to build inclusive and trusted ID systems to empower people and help achieve the Sustainable Development Goals (SDGs). As of 2018, 1 billion people lacked an officially recognized ID, many of whom are marginalized or vulnerable. Barriers to obtaining IDs include high registration costs, discriminatory laws, and bureaucratic inefficiencies (ID4D, 2022). These literary works are about the benefits of national ID programs and their pros and cons. But, they failed to touch upon the cybersecurity governance aspects of these programs. They didn't, especially, mention anything about the challenges these programs face like strategic alignment with general objectives, leadership commitment, resource allocation, legal and regulatory enforcement & accountability.

National ID cards face significant security concerns, such as vulnerabilities from human error during data entry, counterfeiting due to weak security features, and falsification of information (Yazeed Alkhurayyif, 2015). Attacks like man-in-the-middle and skimming can compromise sensitive data, and the centralization of citizen data creates an attractive target for hackers. Misuse by authorized personnel and risks from lost or stolen cards further complicate security. These challenges underline the need for stronger security measures, including biometrics and encryption. (JACOB, 2018) highlights both the benefits of national ID systems, like improved services and safety, and the risks, such as privacy violations, crime prevention doubts, and high implementation costs, stressing the need for a balance between state interests and individual rights. These studies discussed the problems that national ID cards are facing security concerns and that national ID systems benefit in addressing these security concerns. But, they haven't seen the importance of a cybersecurity governance framework for these systems to deal with these problems and the challenges like resource allocation, leadership oversight, strategic alignment, and legal & regulatory enforcement and accountability.

Digital identification systems in East Africa, such as Ethiopia's Fayda and Uganda's Ndaga Muntu, aim to improve access to government services and meet Sustainable Development Goals (SAIIA,

2025). These systems utilize biometric data for security and fraud reduction but face challenges regarding data privacy, exclusion of vulnerable populations, and inadequate legal frameworks. The ITU-T Focus Group Digital Financial Services (FG DFS, 2016) reviewed 67 national identity programs across 43 countries, showing their expansion into services like taxation and healthcare. While these programs enhance efficiency, they encounter issues related to accountability, privacy, and data management. Recommendations for success include transparent implementation and robust cybersecurity measures. These literary works generally talk about the expansion and importance of national ID programs, but they don't mention anything about what kind of cybersecurity governance framework is employed to address challenges like strategic alignment with general goals of the systems, the leadership commitment, resource allocation to the systems, and so on.

The Ethiopian Digital ID Bill raises concerns regarding legal enforcement, accountability, and regulatory oversight due to ambiguities about the roles of various entities and the broad powers granted to the Institute (Yilma, 2022). The delegation of significant legislative authority to subsidiary laws risks undermining democratic processes and increasing discretion for unelected officials, thus reducing accountability. Additionally, the Bill lacks strong data protection measures, exacerbating privacy concerns, especially regarding privatization and third-party involvement. The absence of a clear data protection framework and an independent authority complicates the regulatory environment, underscoring the need for stronger legal safeguards before the Bill is passed. In comparison, Kenya's National Integrated Identity Management System (NIIMS) benefits from a supportive legal structure but requires further refinements, including a standalone digital identity law and amendments to the Data Protection Act 2019, to align with international data protection principles (Kabata, February 2024). These studies put in a vivid manner that legal and regulatory frameworks lack enforcement and accountability seen in national ID programs. However, they failed to include other cybersecurity governance challenges of national IDs are facing such as strategic alignment with general goals, resource allocation issues, leadership commitment problems, and the like.

ENIDP faces several challenges typical of low- and middle-income countries, including issues of enrollment, coverage, accountability, data management, privacy, and costs (Leigh, 2017). While the program seeks to enhance governance, financial inclusion, and service delivery, it faces

persistent hurdles like data privacy concerns, high implementation costs, and limited resources (Ethiopian Business Review, 2024). Regional differences, such as those observed in Sub-Saharan Africa and the Middle East, further complicate efforts to achieve comprehensive national coverage (Tomas, 2022). Despite the program's alignment with successful models like Singapore's NID and India's Aadhaar, the literature fails to address cybersecurity governance challenges. A robust cybersecurity framework is essential to safeguard data, ensure accountability, and protect personal information within ENIDP's digital identity system ((citizenshiprightsafrica, 2023); (MOSIP, 2023)). Albeit these works studied issues in realtion to ENIDP's lack of inclusivity, privacy problems, and the like and the pivotal role cybersecurity framework plays, they didn't discuss the importance of cybersecurity governace framework to address paramount challenges like cybersecurity strategic alignment with overall goals, leadership oversight, allocation resources and enforcement and accountability of legal and regulatory frameworks.

Thus, this thesis aims to study and enhance the cybersecurity governance aspect of the ENIDP by analyzing the five cybersecurity governance challenges; strategic alignment, senior leadership's commitment, standardized processes, enforcement and accountability and resources (Hedges, 2019) (Badi, 2020). By analyzing the existing practices within the ENIDP, we have proposed a comprehensive cybersecurity governance framework designed to align the program's cybersecurity strategy with its overarching business objectives. This framework emphasizes leveraging senior leadership's commitment, enforcing legal and regulatory frameworks, establishing clear accountability mechanisms, and ensuring the effective allocation of resources. The primary goals are to strengthen data protection, implement advanced security measures, and achieve compliance with both international standards and national cybersecurity policies and laws. Ultimately, the framework aims to create a robust system that mitigates risks, fosters public trust, and ensures the ENIDP's effectiveness, security, and long-term sustainability.

1.4. Research Questions

The research questions of the thesis are:

1. To what degree do the ENIDP's cybersecurity strategy and goals align with its business objectives?

2. To what extent is senior leadership committed to providing strategic oversight and guidance for the organization's cybersecurity program?
3. What are the most common challenges that ENIDP faces in implementing standardized processes for cybersecurity governance?
4. How are enforcement and accountability controls implemented to facilitate compliance with relevant legal and regulatory cybersecurity frameworks?
5. What factor influences the decision of the allocation of resources for cybersecurity programs?

1.5. Objective of the Study

In this section, both the general objective and specific objectives of the research are stated clearly and succinctly.

1.5.1. General Objective

The general objective of this research is to study ENIDP's cybersecurity governance aspect and propose a cybersecurity governance framework for digital identification programs.

1.5.2. Specific Objectives

The specific objectives of the research are:

1. To study the cybersecurity governance challenges in ENIDP, specifically focusing on strategic alignment, senior leadership commitment, standard processes, enforcement and accountability mechanisms, and resource allocation.
2. To develop a cybersecurity governance framework particularly to improve the security posture of the ENIDP.
3. To evaluate and validate the effectiveness and usability of the propposed cybersecurity governance framework.

1.6. Expected Contribution of the Study

This study addresses a gap in the research on the integration of cybersecurity governance with national identification systems, proposing a foundational framework to secure digital ID programs.

It offers a scientific contribution by providing an initial model for future researchers to develop advanced cybersecurity governance frameworks. Practically, it contributes a context-specific cybersecurity governance framework tailored to digital identity systems, offering organizations a roadmap to enhance security and manage risks. The study also lays the groundwork for case studies and empirical research to validate the framework, urging further exploration in this critical area of cybersecurity for national digital identification programs.

1.7. Scope of the Study

The scope of this research is focused on studying the cybersecurity governance aspects of the ENIDP relating to strategic alignment, senior leadership oversight, enforcement and accountability, standardized processes, and resources. Furthermore, the study involves the development of a cybersecurity governance framework aimed at enhancing the overall security of the program.

1.8. Structure of the Document

This document is organized into six main chapters. chapter one is the introductory part, comprising the introduction, background of the study, motivation for the study, statement of the problem, research questions, objectives of the study, expected contribution of the study, the scope of the study, and the structure of the document. Chapter two covers the literature review, which reviews various literary works related to the research topic. This section includes an introduction to the literature review, the approach used an examination of the adoption of digital identity programs by different countries, the problems associated with using an open-source platform, a review of extant information, cybersecurity and IT frameworks, and a discussion of cybersecurity issues in digital identity programs and cybersecurity governance. Related works and the conceptual framework are also discussed. Chapter three details the research design and methodology, including the research design, population and sampling design, key informants, data sources, data collection methods (in-depth interviews and document analysis), data analysis techniques, and quality criteria such as reliability, replicability, validity, and generalizability. Ethical considerations are also covered in this section. Chapter four presents the data analysis and interpretation of results, including qualitative data analysis techniques, thematic analysis, interview transcriptions, and information about the respondents. Chapter five discusses the

findings, providing an introduction, a presentation of the results, and a discussion of the thematic analysis results with conclusions and recommendations based on the research findings. The final chapter, chapter six, presents the proposed cybersecurity governance framework. Additionally, it includes principles, key performance indicator, high level framework implementation guide, framework validation, limitation and future work.

Chapter-Two: Literature Review and Related Works

2. Literature Review

2.1. Introduction

Identity is the answer to the question, 'Who am I' (Erikson, 1994). It has various meanings today, some simply referring to social categories or roles and others to basic information about oneself (Turner, 2018) whereas national identity is a person´s identity or sense of belonging to one state or one nation (Erikson, 1994), (Ibid). The traditional identity systems have been based on face-to-face interactions, on physical documents and processes which do not meet the needs of current

society due to the transformation from analog to digital (Matthew N.O. Sadiku, 2016), (MIT, 2016). The digitalization of government services and business taking place online required the need to have electronic representation of individuals and entities claiming who they are. A digital Identity is an electronic representation of the information on a person, organization, or object that is identical to the real identity of a person or entity (Matthew N.O. Sadiku, 2016). A national digital identity consists of different elements of unique identifiers such as name, date of birth, audio information in the form of a voice sample, biometric data such as blood samples, iris scans, fingerprints, and hair samples, descriptive information such as physical traits, including weight and height, personal identifiers like a US Social Security number (SSN) or any government-issued identifying number…etc. to identify citizens. However, the application of these elements differs from country to country (Gavendra Singh, 2017). An individual's identity and reliability are proven via the national digital identification system during any transaction or encounter, whether online or in person. It is an essential tool that governments and both public and private businesses can use to identify every person and evaluate that person's actions when utilizing services (e.g., social welfare, financial support). By accurately and effectively providing government services and lowering the possibility of human error when identifying and authenticating an individual, it helps to meet people's requirements and improves a country's overall efficiency (Gavendra Singh, 2017).

2.2. Literature Review Approach

In this part of the research, a deep analysis of existing related literature is done using a systematic literature review approach. This literature review is not only done in this chapter but also throughout the rest of the chapters. The approach the researcher follows is illustrated in the figure below which is adapted from (Scott Ainslie, 2023) and which is in turn adapted from (Tuure Tuunanen, 2007).

The steps mentioned in the approach are: Step 1) define the search approach, Step 2) identify relevant literature in leading journals and conference proceedings using a search engine, Step 3) use backward chaining – review the citations used by the papers identified in Step 1, and Step 4) use forward chaining – identify articles that cite these papers, and Step 5) where we get the total number of literature after the searching and filtering process is over.

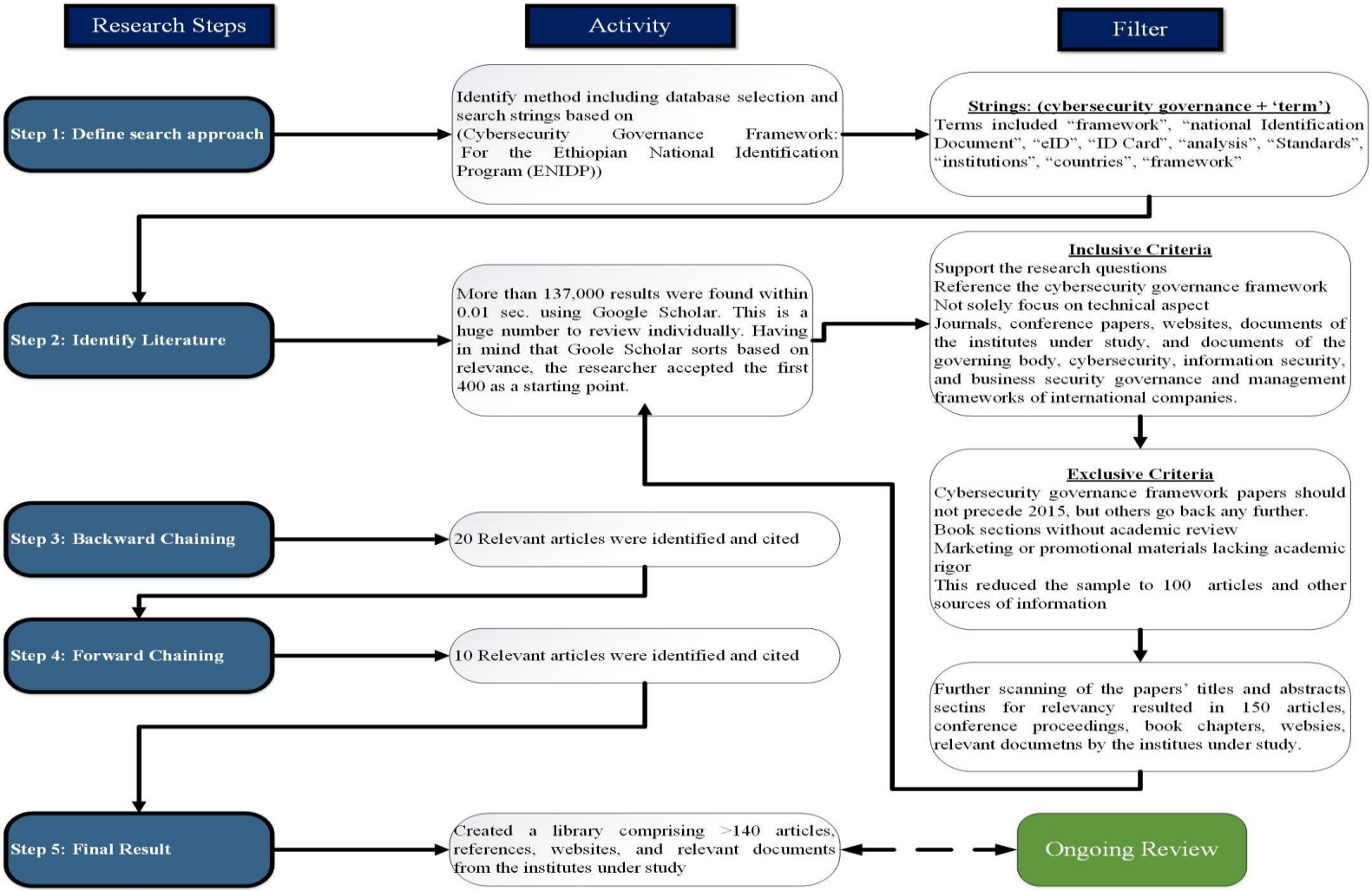

Figure 2-1: Literature Review Approach

2.3. The Adoption of Digital Identity Programs by Different Countries

Several countries in the world understand the importance and necessity of adopting a national digital identity program. Estonia has one of the best-integrated national digital identity systems called eID. It was launched by the public sector in 2000 with over 940 public and private sector institutions connected today (Olivia White, 2019). Estonians use their eID via ID-card which is used as proof of ID in an electronic environment; Mobile-ID on their smartphones allowing to access secure e-services and digitally sign documents; or via the application Smart-ID, a smartphone without a dedicated SIM card that is used to prove their identity virtually and applied in financial sector e-services as well as confirms transactions and agreements. In addition, Estonia has an e-residency for a borderless digital society for global citizens (e-Identity, 2024). Likewise, China has a well-integrated digital ID card as a national digital identification system that gives citizens access to hotels, ticketing, bank services, delivery services registering for government services, and so on. This virtual ID card is part of the popular messenger service WeChat. To curb online identity theft, facial recognition is used to verify users before the virtual ID is authorized in the app (Singh P. , 2022). The United Kingdom uses a national digital identity system to simplify different government services for its citizens, such as obtaining tax refunds, pensions, and mortgages (Taylor, 2021). Canadians' digital identities are distributed systems launched in 2012 that are led and operated by financial institutions. It enables authentication only with a range of public and private sector institutions through online login (Olivia White, 2019). In Singapore, each citizen must obtain a national identity card called Singpass at the age of 15 through which citizens can then access online services offered by the government (ICA, 2024). Similarly, BankID Sweden was launched in 2003 by financial institutions, now recognized by the government. It enables digital authentication and signature with limited data sharing for use with public and private sector institutions through smart cards or digital devices (Olivia White, 2019). The Digital Identification System of Argentina is launched by the government in coordination with the private sector. It enables remote biometric authentication across the public and private sectors. The Nigerian's National eID card, on the other hand, was launched by the public sector in partnership with MasterCard in 2014 and enables authentication through chip-based card and data sharing for KYC (Know Your Customer) with potential additional future use cases under consideration. The Aadhaar India, launched in 2009 by agency established by public sector and enables biometric

digital authentication as part of broader digital ecosystems with additional functionality. Key use cases include direct transfer of benefits to bank accounts, e-KYC, and digital document storage (Olivia White, 2019).

2.4. The Problems of Using an Open-Source Platform

Open-source software simplifies development for both developers and third-party vendors but also exposes vulnerabilities due to its open nature. Once attackers identify a flaw, they can exploit it for data breaches, Denial of Service (DoS) attacks, or even ransomware incidents (Maayan, 2019). Risks associated with open-source platforms include unpatched vulnerabilities, compromised dependencies, outdated components, and regulatory issues (Kaminsky, 2023). National identity systems like MOSIP, eID, Login.gov, and GOV.UK Verify rely on open-source frameworks. Security assessments of MOSIP highlight risks in registration modules, including insecure protocols and susceptibility to SQL injection and man-in-the-middle attacks (Waris Aiemworawutikul, December 2019). While the EU's eID ensures secure cross-border verification, it lacks adaptability for developing regions. Similarly, Login.gov enhances authentication but raises privacy concerns due to transaction tracking. In contrast, GOV.UK Verify prioritizes unlinkability to protect user privacy, though further transparency in data sharing could enhance security (ibid).

2.5. Review of Extant Information, Cybersecurity and IT Frameworks

The digital threat landscape constantly evolves, with malicious actors launching more sophisticated attacks daily. Organizations must take account of the latest security frameworks to stay ahead of this dynamic threat environment (Ryerse, 2023). Cybersecurity frameworks provide an organized approach to managing security risks, mitigating potential vulnerabilities, and improving overall digital defense. As enterprises continue integrating digital technologies into their operations, staying up-to-date with the most current cybersecurity frameworks is increasingly important. From the National Institute of Standards and Technology (NIST) to the Health Insurance Portability and Accountability Act (HIPAA), cybersecurity frameworks are an essential part of any IT operation.

In the NIST glossary, the term cybersecurity framework is defined as, "*A risk-based approach to reducing cybersecurity risk composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers*." A cybersecurity framework is a set of policies, practices, and procedures implemented to create an effective security posture. These frameworks provide organizations with the guidance to protect their assets from cyber threats by identifying, assessing, and managing risks that could lead to data breaches, system outages, or other disruptions. Cybersecurity frameworks help organizations develop and maintain an effective security strategy that meets the specific needs of their environment. Through evaluating current security practices and identifying gaps in protection, these frameworks help cybersecurity teams implement appropriate safeguards to protect critical assets. It is described (Cisternelli, 2024) that the cybersecurity framework provides a common language and set of standards for security leaders across countries and industries to understand their security postures and those of their vendors. On the other hand in (CISCO, 2024) the term cybersecurity framework is defined as "*The Cybersecurity Framework (CSF) is a set of cybersecurity best practices and recommendations from the National Institute of Standards and Technology (NIST). The CSF makes it easier to understand cyber risks and improve your defenses. Organizations around the world use it to make better risk-based investment decisions."* From the above subsequent definitions, we can deduce that CSF is a guideline for us to deal with cyber risks and help our organization in achieving its core objectives.

Overall in this section, the researcher made a thorough and a meticulous discussion on four cybersecurity frameworks that are related to cybersecurity governance and management. Cybersecurity governance is a comprehensive cybersecurity strategy that integrates with organizational operations and prevents the interruption of activities due to cyber threats or attacks (CISA, 2024). Features of cybersecurity governance include: 1) accountability frameworks, 2) decision-making hierarchies, 3) defined risks related to business objectives, 4) mitigation plans and strategies, and 5) oversight processes and procedures.

2.5.1. National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology (NIST) is a governmental agency responsible for advancing technology and security standards within the United States. NIST's Cybersecurity Framework provides guidelines for organizations to identify, protect, detect,

respond to, and recover from cyber-attacks. The framework was created in 2014 as guidance for federal agencies, but the principles apply to almost any organization seeking to build a secure digital environment.

The **NIST Cybersecurity Framework** was established in response to an executive order by former President Obama — Improving Critical Infrastructure Cybersecurity — which called for greater collaboration between the public and private sectors for identifying, assessing, and managing cyber risk. While compliance is voluntary, NIST has become the gold standard for assessing cybersecurity maturity, identifying security gaps, and meeting cybersecurity regulations.

Now in its second version, NIST's framework is a comprehensive set of best practices for organizations looking to improve their security posture. A noteworthy addition to this edition is the emphasis on cybersecurity governance, which acknowledges cybersecurity as a crucial element of enterprise risk management alongside other issues. It includes detailed guidance on risk management, asset management, identity and access control, incident response planning, supply chain management, and more. The figure illustrated below manifests the various elements of the framework.

Figure 2-2: The NIST Cybersecurity Framework

[Source: BITSIGHT]

2.5.2. ISO/IEC 27014: 2020

ISO/IEC 27014:2020 guides the governance of information security, enabling organizations to evaluate, direct, monitor, and communicate information security-related processes (Schirn, 2024). It targets the governing body, top management, and those responsible for overseeing an ISMS based on ISO/IEC 27001, as well as those managing information security outside the ISMS scope but within governance. This standard ensures that information security processes align with organizational objectives and governance requirements.

2.5.3. COBIT 5 and COBIT 2019

COBIT® (Control Objectives for Information and Related Technology) is a comprehensive framework designed to support the management and governance of enterprise IT (EGIT). It outlines the components and design factors necessary for creating and maintaining an effective governance system. First released in 1996, the latest version, COBIT 2019, was introduced in 2018 to incorporate new technology and business trends, such as digitization, and to update COBIT 5, which was published in 2012 (Harisaiprasad, 2020). COBIT 2019 includes new insights from IT and governance experts, and understanding the key differences between COBIT 5 and COBIT 2019 is crucial for a smooth transition.

Developed by the Information Systems Audit and Control Association (ISACA), it is a comprehensive framework designed to help organizations manage their IT resources more effectively. This framework offers best practices for governance, risk management, and security. The COBIT framework is divided into five categories: Plan & Organize, Acquire & Implement, Deliver & Support, Monitor & Evaluate, and Manage & Assess. Each category contains specific processes and activities to help organizations manage their IT resources effectively. It also includes detailed data security and protection guidelines, covering access control, user authentication, encryption, audit logging, and incident response areas. These guidelines provide organizations with a comprehensive set of measures that can be used to protect their systems from cyber threats.

COBIT 2019 introduces six governance system principles, one more than the five in COBIT 5, to ensure stakeholder needs are evaluated, and agreed upon based on enterprise objectives, set direction through prioritization and decision-making, and monitor performance and compliance. Additionally, COBIT 2019 revises some of the terminologies used in defining these principles.

Despite these changes, the governance and management objectives remain similar between COBIT 5 and COBIT 2019. See the figure below.

Figure 2-3: Governance and Management Objectives in COBIT 5 and COBIT 2019

[Source: ISACA]

The figure shown below clearly manifests the COBIT 5 and COBIT 2019 principles.

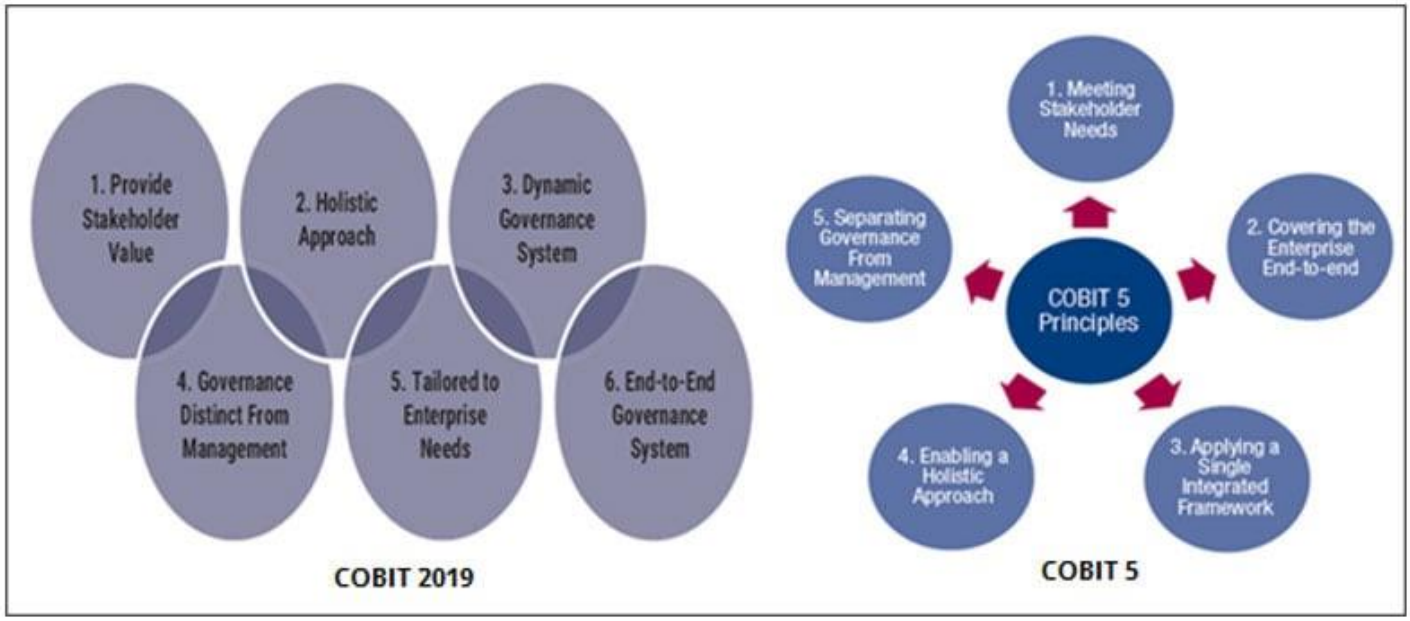

Figure 2-4: Governance Principles in COBIT 2019 and COBIT 5

[Source: ISACA]

From Figure 2-4 one can see that there are 6 governance system principles in COBIT 2019, as compared to 5 in COBIT 5. Governance principles exist to ensure that stakeholder needs are

evaluated and agreed on based on enterprise objectives, to set direction through prioritization and decision-making, and to monitor performance and compliance against the set direction and objectives (ibid). Generally, the table shown below compares and contrasts COBIT 5 and COBIT 2019.

Table 2-1: Key Differences Between COBIT 5 and COBIT 2019

Feature	COBIT 5	COBIT 2019
Governance Principles	Five governance principles	Six governance principles
Processes	37 processes	40 processes
Terminology for Management Processes	"Manage" terminology	"Managed" terminology
Terminology for Governance Processes	"Ensure" terminology	"Ensured" terminology
Governance Framework Principles	Absent	Added
Performance Measurement	0-5 scale based on ISO/IEC 33000	CMMI performance management scheme
Enablers	Included	Renamed as components
Design Factors	Not available	Included

The table above shows that more changes can be noted in the processes that support the governance and management objectives. The number of processes is increased, from 37 in COBIT 5 to 40 in COBIT 2019. The terminology has also changed slightly, from the use of the verb “manage” in COBIT 5 to the adjective “managed” in COBIT 2019.

The COBIT framework is crucial for businesses to effectively govern and manage their IT departments. By aligning IT processes with business goals, COBIT ensures optimal resource utilization and risk mitigation, leading to cost savings in IT services. COBIT 5 enhances this by allowing businesses to track information assets with advanced methods, facilitating better decision-making and industry survival. Certified COBIT 5 Assessors and Implementers help businesses apply the framework to streamline IT and business processes, balancing risk management with IT governance through its five foundational principles (JONES, 2022). These principles are applicable across various business sizes and sectors. COBIT 5 is founded on five

principles essential for effective IT management and governance: meeting stakeholder needs, covering the enterprise end-to-end, applying a single integrated framework, enabling a holistic approach, and separating governance from management (IT Governance Ltd , 2024). These principles, supported by seven enablers—people, policies and frameworks; processes; organizational structures; culture, ethics, and behavior; information; services, infrastructure, and applications; and people, skills, and competencies—allow organizations to align IT investments with their objectives, ensuring they realize the value of those investments.

2.5.4. Information Technology Infrastructure Library (ITIL)

ITIL is a widely adopted framework that standardizes IT service management (ITSM) to enhance efficiency and align IT operations with business objectives (Bigelow, 2024). Introduced in 1989, ITIL has evolved through multiple versions, with ITIL v2 refining service support and delivery, ITIL v3 expanding into service strategy and continual improvement, and ITIL 4 integrating modern methodologies like DevOps to address digital transformation needs. ITIL 4 introduces four dimensions of service management and 34 practices, ensuring adaptability in a service-driven economy. The transition from ITIL v3 to ITIL 4 also updated the seven guiding principles, reinforcing their role in decision-making and continuous improvement (QRP, 2021). They guiding principles are discussed in the table below.

Table 2-2 Guiding Principles of ITIL

Guiding Principle	Description
Focus on value	Emphasizes delivering value to customers and stakeholders, aligning services with business needs.
Start where you are	Encourages organizations to begin improvement efforts from their current position and capabilities.
Progress iteratively with feedback	Suggests making continual progress through iterative cycles, incorporating feedback for improvement.
Collaborate and promote visibility	Promotes collaboration across teams and departments, ensuring transparency and visibility in processes.
Think and work holistically	Encourages considering the interconnectedness of processes and systems, taking a holistic approach to service management.

Keep it simple and practical	Advocates for simplicity and practicality in solutions and processes to minimize complexity and improve efficiency.
Optimize and automate	Focuses on optimizing processes and automating tasks to enhance efficiency and effectiveness.

The figure shown below illustrates the 7 principles in a clear and succinct manner.

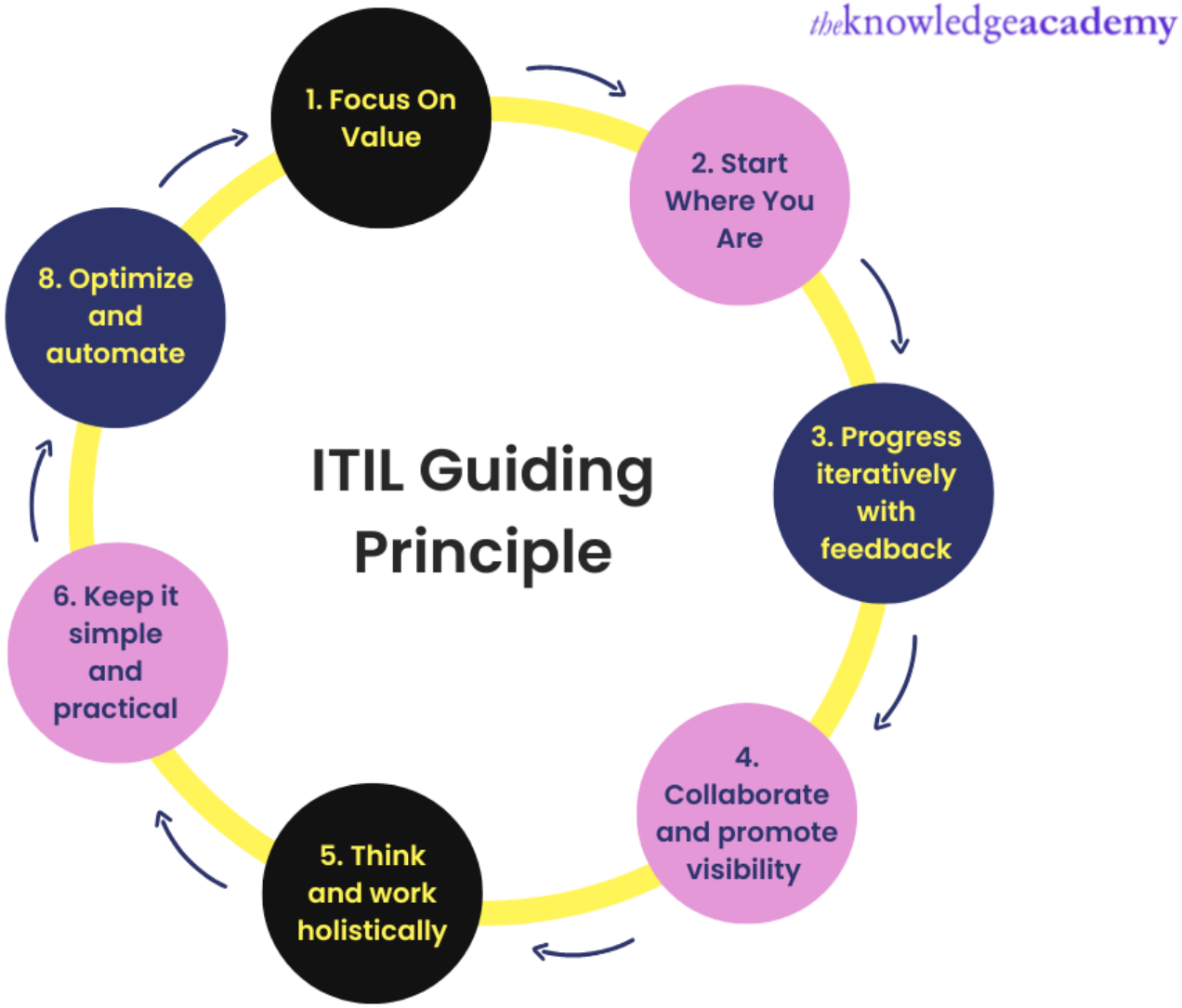

Figure 2-5 ITIL Guiding Principles

[Source: theknowledgeacademy]

2.5.5. A Dynamic and Adaptive Cybersecurity Governance Framework

The author (Melaku, 2023) delved into an exhaustive examination of existing IT and security governance frameworks, spotlighting their intricate nature and associated limitations, such as high costs and resource demands. In response to these challenges, the author proposed a straightforward, dynamic, and adaptable cybersecurity governance framework, aimed at offering strategic direction for security management, ensuring efficient risk mitigation, and optimizing resource allocation. The framework's core components, activities, outcomes, and processes are delineated, accompanied by the introduction of key performance indicators (KPIs) to gauge its effectiveness. The depicted figure, Figure 2 6, shows the proposed framework.

The proposed cybersecurity governance framework emphasizes flexibility, a risk-based approach, alignment with standards and compliance, a holistic approach, separation of governance from management, an adaptive governance structure, tailoring to enterprise needs, fostering a cybersecurity culture, an end-to-end governance system, and cross-sector collaboration as principles. This framework promotes adaptability, compliance, and holistic security management while emphasizing tailored approaches and fostering a security-aware culture to address evolving threats. Additionally, the study identifies four key KPIs: financial metrics to assess cost-effectiveness, operational metrics to evaluate performance, maturity assessment metrics to gauge security control maturity, and benchmarking to compare against industry standards. These priciples and KPIs help organizations measure, improve and optimize their security programs effectively.

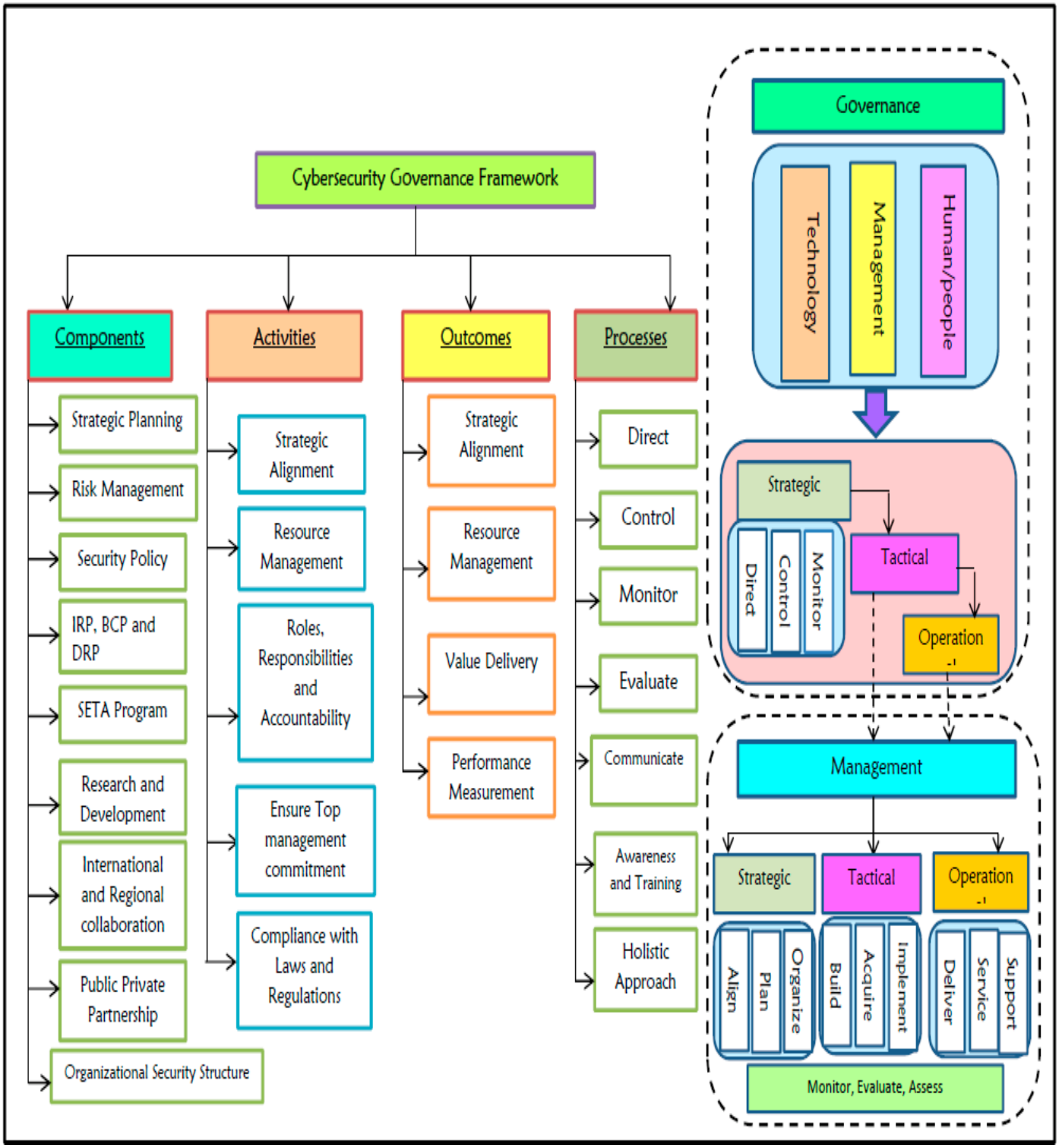

Figure 2-6 A Dynamic and Adaptive CS Governance Framework

[Source: Melaku, 2023]

Table 2-3 Comparative Analysis of Selected Cybersecurity Governance Frameworks

Parameter	NIST Cybersecurity Framework	ISO/IEC 27014:2020	COBIT 5 and COBIT 2019	Information Technology Infrastructure Library (ITIL)	Dynamic and Adaptive Cybersecurity Governance Framework
Applicability	Cross-sector, primarily US	Global	Global	Global	Global
Focus	Risk-based cybersecurity	Information security	IT governance and management	IT service management	Adaptive cybersecurity governance
Domain	Cybersecurity	Information security	IT Governance	IT service management	Cybersecurity governance
Implementation	Flexible framework	Guideline	Framework	Framework	Dynamic and adaptive framework
Scope	Cybersecurity practices	Information security	IT processes	IT service delivery processes	Comprehensive cybersecurity governance
Ownership	National Institute of Standards and Technology (NIST)	ISO/IEC JTC 1/SC 27	ISACA	Axelos Ltd.	Organization implementing framework
Main Usage	Improving cybersecurity risk management and resilience	Governance guidance	IT governance alignment	IT service management improvement	Adapting to evolving cybersecurity threats and challenges

Issuer	NIST	ISO/IEC	ISACA	Axelos Ltd.	Organization implementing framework
Integration with other frameworks	Integrated with existing cybersecurity risk management processes	Complements ISO/IEC 27001	Integration with ITIL	Often integrated with other IT management frameworks	Can be integrated with existing governance frameworks

2.6. Cybersecurity Issues in Digital Identity Program

The transition to a digital economy, and having online transactions and data requires a secure identity system with enhanced privacy. Identity theft, data breaches, and large-scale fraud are all on the rise (MIT DIGITAL, 2016). The issue with such a system is in its operational and architectural components, as well as in its state-wide pervasiveness, the concentration of personal data, persistent records of various activities, and the impossibility of withdrawal (Renata M. de Carvalho, 2020). Technology has brought us several benefits that ease our day-to-day lives. Any interconnectivity throughout the digital world, if not managed well, could cause us to fall into a cyber risk. According to (Olivia White, 2019), the digital ID, which supports the digital economy, is susceptible to all current cyber risks, just like any other digital technology that is widely used by the general public. National Digital ID is sensitive and if a security compromisation occurs the repercussions are severe. Potential risks are also presented by the connectivity and information residing in digital ID systems, processes, and procedures. Data leaks, issues related to hardware, software, and infrastructure as well as improper control and misuse of personal data are the associated probable risks related to the digital ecosystem.

The increase in the application of digital services is leading to generalized concerns about privacy. In the citizen's identification system, citizens' data is processed by all entities including third parties (Renata M. de Carvalho, 2020). The collection, processing, and disclosure of information by the individual's consent do not impose on their privacy. However, sharing of secret information,

use of information beyond what it is intended for, information linking across domains, etc. negatively impacts privacy (Cofta, 2008).

From the information security perspective, individuals' or citizens' data is vulnerable by being kept in a central database. And with the assumption of having a long operational lifespan and motivations for attacking such systems, one can assume that the database will be compromised regardless of technical countermeasures taken (Ibid). Without proper controls, digital ID system administrators with nefarious aims would gain access to and control over data. As a result, there will be a misuse of the identification programs (Ibid).

.One of the causes for a cyber-risk can be improper design or operation of the Digital ID system which can directly affect individuals becoming the victim of identity theft or their civil rights can be restricted if it is used as a means to cross-link surveillance systems. Privacy as well as other personal rights can be significantly violated either as a result of deliberate information sharing or by direct attack on the system (Ibid).

A wide range of security issues can result in national threats and the loss of data confidentiality, integrity, and availability in an online environment due to the unpredictable and dynamic cybersecurity landscape. By resulting in online privacy violations, terrorism, and corruption, security risks can jeopardize the current national and social conditions. Some of the cyber risks related to the national digital identity systems are centralized data storage risk, Biometric risk, mass-surveillance risk, and exclusion. A central national digital identity database creates a single point of failure if a cyber-attack occurs. The biometrics data, the main aspect of personally identifiable information, is sensitive; and if it is leaked, it is irreversible and any misuse of such information will affect the individual's reputation. The authentication and verification service given by the national digital identity system in one place increases the opportunity for mass surveillance and profiling simply by analyzing logs over time. The exclusion risk transpires when malicious internal or external actors change digital identity details, hence excluding the individual from accessing services or receiving benefits (Gavendra Singh, 2017).

2.7. Related Works

2.7.1. Cybersecurity Governance

The capacity to thwart and recover from cyberattacks can be referred to as cybersecurity. There are several definitions provided by different international standards and frameworks; The International Telecommunication Union (ITU) (ITU-T X.1205, 2024) defined Cybersecurity as "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment." The National Institute of Standards and Technology (NIST), which is in charge of defining technical terms used by the US government, has four definitions of cybersecurity (Security Scientist, 2024) and the one they put first place is "the prevention of damage to, unauthorized use of, exploitation of, and – if needed – the restoration of electronic information and communications systems and the information they contain, to strengthen the confidentiality, integrity, and availability of these systems." the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC 27032) (ISO, 2024) addressed "Cybersecurity" or "Cyberspace security" as the "preservation of confidentiality, integrity, and availability of information in the Cyberspace" and the term "Cyberspace" is defined as "the complex environment resulting from the interaction of people, software, and services on the Internet employing technology devices and networks connected to it, which does not exist in any physical form."

With the big picture of an enterprise, Corporate Governance (CG) represents the area for achieving a company's goals which encompass any management domain that can sustain the company's long-term success with the objective of effective and secure business performance. The part of corporate governance that strategically handles risks related to cybersecurity is referred to as cybersecurity governance (Pullin, 2018). According to the study (Eugen, 2018), cybersecurity governance is a

subset of Corporate Governance which refers to all managerial domains that might help an organization realize its goals and assure its long-term success. Cyber risk can be eliminated or minimized through the effective implementation of a cybersecurity strategy. Such implementation of strategy can be achieved by introducing the concept of cyber governance (Karataş, 2022) . A sound cybersecurity governance system will assure that the organization's cybersecurity program aligns with its business objectives. In addition to helping the business meet its cybersecurity and risk management objectives, good governance will offer a strategic perspective on how enterprise security is managed (Ibid).

The primary objective of cybersecurity governance is attained through predetermined goals in the form of cyber policies and procedures that are established by cybersecurity governance (Hafeez-Baig, 2021). It is an essential component of corporate governance due to the extensive transition to cyberspace. The business corporation that adopts cybersecurity governance, adheres to clear, sound, and transparent principles, rules, regulations, and processes, and implements staff awareness and training programs (Badi, 2020). Traditionally, the technical and IT department handles the management of security issues and information systems, however more recently, the non-technical and C-suite levels have been added to the ranks of individuals who are now in charge of cybersecurity and cyber risk. Thus, the influencers and decision-makers inside an organization, as well as daily desk workers, are accountable for cybersecurity (RSA, 2016)

To achieve effective governance of cybersecurity for corporations, it is essential to integrate three main elements: processes, technology, and persons (Badi S. A., 2020). Processes are the regulatory measures that identify and show how to use a variety of regulatory activities, procedures, roles, and documents to minimize risks posing a threat to a corporation's information. Regulatory measures are already set up to define roles, policies, and other elements of operations. They give us the requirements we need to apply standards without any further difficulties or expenses. Cybersecurity Strategy, Cybersecurity Management, Cybersecurity Policies and Procedures, Management of Cybersecurity Risks as well as Compliance and Control are some of the themes constituted under the process element. Technology, on the other hand, is the application of technological tools, software, and devices for the effectiveness of cybersecurity and mitigating risk. The last element, people constitutes the need for capacity building for individuals through

continuous, efficient, and effective cybersecurity awareness and training programs (IT Governance Ltd, 2024).

There are challenges that business corporations may face when implementing the cybersecurity governance program. These challenges are related to cybersecurity strategy, unified/ standardized processes, implementation/ enforcement and accountability, senior leadership control, and resource (Hedges, 2019) (Badi, 2020).

2.7.1.1. Cybersecurity Strategy

The cybersecurity strategy challenge for the governance program is due to its construction without assessing the possible cybersecurity risk. For good cybersecurity governance, the creation of a cybersecurity strategy should come after a good definition and implementation of a cybersecurity risk management approach with a clear set of objectives (Ibid)(Ibid). Cybersecurity strategies must be flexible to enable the adaption of future changes, whilst being thoroughly examined to ensure that they are pertinent to organizational workflows and knowledge gaps (Alina, 2016), (Boutwell, 2019). It should be a high-level document that establishes the roadmap for the organization to encompass the definition of cybersecurity scope, identification of cybersecurity needs and objectives, establishing of key performance indicators, resource needs, risk appetite, continuous monitoring and evaluation, organizational culture, and the human factor (Ibid) (Ibid).

2.7.1.2. Unified/ Standardized Processes

Every organization has specific processes and procedures for carrying out its duties. The problem with cyber governance is when a unified or standardized process is absent throughout the work that ensures efficiency, quality, or consistency. Constancy is often necessary for a common understanding and management approach to risk; a reproducible procedure can improve the cybersecurity management program. As a result, its absence could increase the likelihood of security breaches, hacks, and attacks (Ibid)(Ibid).

2.7.1.3. Implementation/ Enforcement and Accountability

Cybersecurity governance should be measurable and practicable and its requirements should be enforced through accountabilities. Accountabilities of personnel through continuous monitoring of the implementation of regulations ensures compliance with policies, procedures, and legal

frameworks. Thus the absence of such accountability and compliance will lead to inconsistency and lack of standardized process, therefore consequences in failure (Ibid)(Ibid).

2.7.1.4. Senior Leadership Control/ Oversight

Since cybersecurity governance is an organization-wide concern, the senior leadership must continually take part in and support the cybersecurity program by providing oversight to guarantee that the process and procedures are accomplishing its goal (Ibid). They also enforce proper behavior by holding people accountable for the evaluation, creation, storage, usage, archiving, and deletion of information. It consists of the procedures, responsibilities, policies, standards, and metrics that guarantee the effective and efficient use of data in assisting an organization in achieving its objectives (Diogo Proen, 2016).

2.7.1.5. Resource Allocation

In general, one of the challenges in cybersecurity programs is top management's limited commitment to allocating and spending resources for cybersecurity. The cybersecurity program is effectively enhanced through considerate funding. The senior management with their decision-making mandate should guarantee enough resources to satisfy the need for cybersecurity governance. Security training for the staff, as well as anything applied to mitigate cyber risk, requires a budget (Ibid).

In general, the digital identity world is far from flawless. The processes involved need to be streamlined through more work. Personal data that belongs to the individual should be governed by their ownership and backed by regulation as part of such streamlining. Therefore, an organization's digital identity strategy and plan must include data governance and privacy. Every applicable legislation, rule, industry standard, and internal policy should be complied with by a digital identification system, particularly those that deal with data privacy, data protection, and fraud prevention (Jan Vanhaecht, 2020).

2.7.2. Evolving Landscapes of Digital Identity: Global Insights and Governance Challenges

Electronic identity systems are transforming the provision of services and citizen engagement globally, particularly in the context of young populations like Indonesia's Generation Z. (Zahlimar, 2023) recognizes that digital ID cards facilitate administration, save the

environment, and are favorably accepted by yund users despite challeges with access and data protection.The same problems exist in Nepal, where biometric National Identity Cards offer government and economic benefits but raise logistical and public trust issues (Diyal, November 2023). (Kim, 2023) discusses how Estonia's e-ID model could influence US policy, with privacy protections, blockchain, and stakeholder acceptance identified as methods to reduce risks and ensure equity of implementation. At the policy level, (Bhandari V. a., 2020) identifies the call for harmonised legal safeguards and enforcement mechanisms within the scope of speeding-up technological change, tracing the direction of privacy and data protection regimes through global case studies.

At a level higher than individual countries, global research shows generalised trends in digital identity uptake. (Jide Edu, 2023) provides a comparative review of NeID systems in Estonia, India, and Australia with efficiency return marked by pressing concerns. Africa lingers as an imposing instance with over 500 million without legal identity, but digital IDs as tools for inclusion and economic empowerment, according to the African Union Digital Transformation Strategy (Gabriella, 2021). These systems are required not just for national development but also for backing of continent-level ventures like the AfCFTA. But their utilization hinges on the resolution of legal, infrastructural, and preparedness elements. A related study by (Bin Srinidhi, 2015) introduces a financial point of view, illustrating that in risky environments like cybersecurity, firms tend to underinvest in productive capital due to risk aversion unless there are external insuarace provisions to align stakeholder incentives better-a lesson that is applicable to government investment in digital IDs.

To evaluate the governance quality of digital ID systems, the Centre for Internet and Society brought about the "Governing ID: Principles for Evaluation" framework (Babikian, February 2024). The instrument uses Rule of Law, Rights-based, and Risk-based tests to establish the legitimacy and accountability of the digital ID architectures. The Rule of Law component addresses legislative transparency, purpose specification, and remedies of redress. The Rights-based tests probe data minimization, access control, exclusionary risks, and necessity. The Risk-based criteria consider proportionality, risk evaluation, and mitigation. The framework was initially used for India's Aadhaar system and has since been applied across ten countries in Africa to assess system integrity and implementation. Together, these studies emphasize that

while digital ID systems can enhance inclusion, service provision, and economic opportunity, their success relies on open governance, sound legal infrastructure, and active stakeholder engagement.

2.7.3. Countries' Expereinces

2.7.3.1. South Africa

The legislative mandate for South Africa's national identity programs is primarily established by the Identification Act of 1997, which grants the Department of Home Affairs (DHA) sole authority over official identity and citizenship (Gabriella Razzano, 2021). However, gaps in this Act regarding biometric data processing led to the enactment of the Protection of Personal Information Act (POPIA) in 2013. South Africa's strong human rights framework supports these laws within an interconnected legal environment, recognizing both historical exclusions and the risks of centralized digital identity expansion (Breckenridge, 2014). While POPIA provides privacy safeguards, ensuring accountability and preventing discriminatory harms will depend on evolving administrative justice mechanisms and sectoral regulations. Recommendations for improvement include risk-based digital identity designs, privacy-by-design principles, and robust public awareness campaigns on data protection (ibid).

2.7.3.2. Lesotho

Lesotho's digital ID system is in the developmental phase, with the National Identity Cards Act of 2011 providing legal grounds for the collection of personal and biometric data for national identity purposes. However, the Act does not clearly articulate the purpose of the digital ID, relying instead on statements from officials (Nthabiseng Pule, 2021). While the system mandates registration for eligible individuals, it risks excluding those unable to register, as it does not allow for alternative forms of identification. Concerns over identity theft persist, despite provisions in the National Identity Cards Act and Data Protection Act to safeguard personal data, as there is no oversight ensuring compliance (Pule, 2021). Researchers have called for various reforms, including advocating for privacy legislation, clarifying the digital ID's purpose, offering alternative biometric options, ensuring data minimization, and introducing mechanisms for transparency, accountability, and grievance redress (ibid).

2.7.3.3. Ghana

Ghana's national ID system is supported by a comprehensive set of laws and regulations, including the Data Protection Act (DPA), and has been strengthened by inclusive measures such as mass registration exercises and the provision of free Ghanacards (Akuetteh, 2021). The National Identification Authority (NIA) has also addressed challenges by setting up registration centers in every district and allowing community vouching for citizens without proof of identity. However, issues remain for the homeless and individuals in slums who struggle to provide reliable digital addresses, potentially affecting the accuracy of their profiles. Despite these efforts, there is a lack of explicit recognition of the national ID as a digital ID, which limits a more focused approach to its digital implications (Akuetteh, 2021). Recommendations for improvement include developing a dedicated policy for digital ID risks, permitting the use of other state-issued IDs, and ensuring inclusivity for marginalized groups (ibid).

2.7.3.4. Zimbabwe

Zimbabwe has yet to fully digitalize its identification system, although some functional digital ID systems exist. These systems have been implemented without a comprehensive legal framework aligned with international human rights laws, leaving citizens vulnerable to potential abuse of their personal data (Nhlanhla Ngwenya, 2021). While the government has introduced a Cyber Security and Data Protection Bill, its provisions are insufficient to fully protect citizens' privacy rights regarding digital IDs. The study recommends enacting an overarching legal framework to ensure transparency and accountability, conducting genuine public consultations for inclusive law formulation, revisiting the Cyber Security and Data Protection Bill, advocating for digital inclusion, and ensuring the participation of women and marginalized groups in the digital ID system (ibid).

2.7.3.5. Mozambique

Mozambique is still in the early stages of developing a fully integrated digital ID system, with ongoing efforts to create digital systems and relevant legislation (Martins P. G., 2021). The e-SIRCEV system shows potential as a foundational basis for a national digital ID, but coordination among the ministries involved is crucial to ensure a holistic approach that addresses citizens' rights, risk mitigation, and implementation challenges. While the 2010 Decree on the Unique Citizen Identification Number (NUIC) provides some framework, the country lacks specific laws

addressing digital IDs, though upcoming laws and regulations will be valuable as the digital ID work progresses (ibid). Recommendations for improvement include enhancing stakeholder coordination, ensuring legislative clarity, promoting regulatory independence, and focusing on system design factors like sustainability, data security, and user-friendliness (ibid).

2.7.3.6. Kenya

In Kenya, the patching of an old colonial law with new digital ID provisions has created gaps, hindering the achievement of a comprehensive and adequate framework, as mandated by the National Integrated Identity Management System (NIIMS) judgment (Grace Mutung'u, 2021). These gaps include the problematic use of executive tools like directives and subsidiary legislation, legal ambiguities in the merging of national ID and digital ID laws, and laws that favor the government (ibid). The study recommends that civil society advocate for digital rights and social justice, considering the profound impacts of digital IDs on identity, inclusion, and governance. Policymakers are urged to ensure broad consultation and phased implementation of digital IDs, while technologists are encouraged to prioritize human rights and propose technologies that foster opportunities, not hinder them (ibid).

2.7.3.7. Rwanda

Rwanda's digital ID ecosystem has been lauded as a model for Africa due to its comprehensive and integrated approach, with over 95% of the population covered by the national population registry (NPR) and online identity verification (Dr. Elvis M. Binda, 2021). The issuance of digital ID cards, alongside the Irembo platform for public service access, has facilitated streamlined identification processes, with private entities like banks benefiting from the NPR database for KYC compliance. However, the legal framework surrounding the use of the national ID remains outdated, lacking provisions for digital ID usage, data protection, and privacy (Dr. Elvis M. Binda, 2021). To address these gaps, it is recommended that Rwanda adopt a comprehensive law on digital ID, strengthen data protection laws, and ensure public awareness of the risks associated with digital identity.

2.7.3.8. Tanzania

Since gaining independence in 1961, Tanzania has strived to provide its citizens with a legal identity, culminating in the establishment of a digital ID system that registers 22 million Tanzanians and issues a unique identifier for life (Patricia Boshe, 2021). This ID enables access to

both online and offline services. However, critical issues remain, including a lack of accountability and transparency in the use of personal data, the centralization of sensitive information with the National Identity Authority (NIDA) without proper transparency mechanisms, and the absence of a comprehensive data protection law (ibid). Additionally, the long-term plan to make NIDA IDs exclusive identity cards could risk excluding citizens from basic services. To improve the system, it is recommended that technologists collaborate with the government and civil society to ensure security, raise public awareness, and update laws to enhance accountability, transparency, and data protection.

2.7.3.9. Uganda

In Uganda, while the ability to own and present legal identification is crucial for government planning, the current registration process under the Registration of Persons Act (ROPA) excludes marginalized groups, particularly the elderly and minority communities (Neema Iyer, 2021). These exclusions result from insufficient stakeholder engagement during the planning stages and inefficiencies in the scoping process. Furthermore, the ROPA lacks safeguards against data breaches and mission creep, and staffing challenges at the National Identification and Registration Authority (NIRA) lead to authentication errors and inadequate applicant notifications, complicating the card acquisition process. To address these issues, it is recommended that civil society advocate for the inclusion of marginalized groups, the government hold public consultations to ensure an equitable ID system, and technologists focus on developing responsible, standardized technology solutions (ibid).

2.7.3.10. Nigeria

Nigeria's digital ID system, while grounded in rule-of-law and rights-based approaches, has significant gaps that expose it to potential human rights abuses. Issues such as vague policies, mandatory enrollment, and the absence of a data protection law and commission could lead to the misuse of the digital ID, harming citizens' rights and excluding vulnerable groups (Babatunde, 2021). To address these concerns, the study recommends that civil society monitor and advocate for the protection of rights, while pushing for the passage of the Data Protection Bill 2020. Policymakers are urged to prioritize data privacy, ensure accountability by amending the NIMC Act, and advocate for the bill’s enactment. Additionally, donor agencies should integrate human

rights dialogue and monitoring into development aid for digital ID projects, recognizing that broader government actions also influence the success of the digital ID initiative (ibid).

Table 2-4 Gaps in the Related Work

Study Title & Author	**Gaps Identified**
"Analysis and Study of the Use of Digital National Identity Card Services in Generation Z" (Zahlimar, 2023).	• Need for improved accessibility, especially for underrepresented groups. • Ongoing data security challenges, requiring better safeguards against breaches. • Lack of research on long-term impacts on identity management and digital inclusion.
"Global Implementation, Impacts, and Challenges of NeID Systems" (Jide Edu, 2023)	• Significant gaps in interoperability across different systems. • Need for inclusive design that considers diverse populations. • Lack of strong legal safeguards to protect user privacy and data.
"National Identity Card (NID) in Bhaktapur, Nepal" (Diyal, November 2023)	• Logistical complexities in implementing a national ID system effectively. • Need for improvements in biometric systems to enhance accuracy and security. • Public trust issues due to lack of transparency and engagement in the process.
"Implementation of National ID in the US, Using Estonia's e-ID as a Benchmark" (Kim, 2023)	• Need for clear and effective rollout strategies to ensure widespread adoption. • Concerns over stakeholder acceptance and collaboration in implementation. • Limited exploration of international implications and comparative lessons.
"Privacy and Data Protection Legal Frameworks in the Digital	• Lack of research on the impact of emerging technologies on existing legal frameworks. • Need for improved effectiveness of compliance mechanisms across different jurisdictions.

Era" (Babikian, February 2024).	
"Resource Allocation between Assets and Security Operations Amidst Cybersecurity Risks" (Bin Srinidhi, 2015)	• Gaps in addressing broader operational risks beyond cybersecurity. • Need for more research on learning effects in decision-making processes among managers.
"Digital Identification in Africa" (Gabriella, 2021)	• Lack of effective governance structures to support implementation. • Need for comprehensive utilization strategies to maximize the impact of digital IDs.
"Evaluation Framework for Digital ID Systems" (Bhandari V. a., 2020)	• Need for application of the evaluation framework to diverse jurisdictions. • Insufficient focus on impact assessment of digital ID systems on users.
"National Identity System (NIS) in South Africa" (Breckenridge, 2014)	• Need for development of risk-based design strategies to mitigate mission creep. • Addressing exclusionary and discriminatory harms that may arise from system implementation. • Insufficient oversight mechanisms to ensure accountability and transparency.
Lesotho (Nthabiseng Pule, 2021).	• Exclusionary practices that impact vulnerable populations must be addressed. • Effectiveness of existing privacy measures needs evaluation. • Insufficient legal framework to prevent data breaches and protect citizens.
South Africa (Gabriella Razzano, 2021)	• Need to address exclusionary and discriminatory harms arising from implementation. • Role of administrative justice in identity management remains unclear.

	• Insufficient focus on the impact of sectoral rollouts on public trust.
Ghana (Akuetteh, 2021).	• Need for clarity regarding digital ID components and data privacy measures. • Potential cybersecurity risks associated with implementation. • Protections for marginalized populations are not adequately addressed.
Zimbabwe (Nhlanhla Ngwenya, 2021).	• Gaps exist between current initiatives and broader digital transformation goals. • Long-term effects of a fragmented legal framework on data protection must be assessed. • Lack of structured oversight raises concerns about accountability.
Mozambique (Martins P. G., 2021).	• Technical, legal, and operational challenges need to be addressed for effective implementation. • Socio-economic impacts of digital exclusion on vulnerable groups remain unexamined. • Privacy risks in the emerging ID landscape require thorough evaluation.
Tanzania (Patricia Boshe, 2021).	• Need for comprehensive assessment of the impact of digital IDs on marginalized populations. • Effectiveness of data protection mechanisms requires further investigation. • Governance improvements in cybersecurity are necessary to protect user data.
Uganda (Neema Iyer, 2021).	• Long-term effects of digital ID exclusion on service access must be analyzed. • Technical performance of the system needs continuous improvement. • Adequacy of data protection laws is crucial for user privacy.

Nigeria (Babatunde, 2021)	• Implications on human rights and inclusion require deeper exploration. • Technical and policy gaps need urgent attention for effective implementation. • Vague policies can increase data protection risks and compromise user privacy.
Kenya (Grace Mutung'u, 2021).	• Stakeholder consultation inadequacies hinder effective policy-making. • Need for empirical research to understand impacts on the population. • Limited focus on external influences affecting implementation success.
Rwanda (Binda, 2021).	• Implications of weak governance structures must be assessed for effectiveness. • Socio-economic impact of data privacy concerns needs exploration. • Updated legal frameworks are necessary to enhance user trust and data protection.

2.8. Research Gaps

Despite the proliferation of cybersecurity frameworks, a notable void exists in the development of research-driven, context-specific governance frameworks, particularly within the realm of national digital identification programs. (Al-Mashhadi, 2023) highlights the significant challenges in implementing cybersecurity frameworks, particularly focusing on their complexity, resource constraints, and the need for customization to fit specific organizational contexts. It emphasizes the difficulties of integrating these frameworks with existing systems, ensuring regulatory compliance, and addressing the skill gaps in cybersecurity expertise. Additionally, the paper underscores the importance of continuous monitoring and updating of cybersecurity measures to adapt to evolving threats. Addressing these challenges is crucial for enhancing the effectiveness of cybersecurity frameworks and protecting organizations from cyber threats.

On the other hand, there is a notable scarcity of literature specifically addressing the cybersecurity governance of national identification programs. While there is substantial research on national identification systems and their technical implementation, as well as general cybersecurity related standards, few studies explicitly combine these areas to explore the governance frameworks necessary to secure national ID programs. This gap in the literature indicates a pressing need for research that develops and evaluates cybersecurity governance frameworks designed to the unique requirements of national identification programs. Such research would help in addressing the evolving cybersecurity threats and ensuring the robustness and resilience of national ID systems.

Chapter-Three: Research Design and Methodology

3. Introduction

In this section, the research design that was followed, the area on which the study focused, the sources of data the research relied upon, the data collection, and the data analysis and interpretation techniques are discussed. The data sources of the research were both primary and secondary. The primary data was elicited using in-depth interviews. The secondary data was garnered from document analysis. That means the research methods that were applied for the study were both an in-depth interview and document analysis. Based on the nature of the research questions, the research methodology was a qualitative research approach that involves "collecting and analyzing non-numerical data (e.g., text, video, or audio) to understand concepts, opinions, or experiences. It can be used to gather in-depth insights into a problem or generate new ideas for research" (Bhandari, 2023).

3.1. Conceptual Framework

A conceptual framework is a structure that researchers believe can best explain the natural progression of the phenomenon under study (Camp, 2001). This framework enables researchers to easily specify and define concepts within research questions (Andy, 2012) . From a statistical perspective, a conceptual framework describes the relationships between the main concepts of research in a logical structure and provides an image or visual representation of how research ideas

are related to each other (Grant, 2015). It graphically or narratively presents the key variables or components under investigation and the presumed relationships between them (Michael, 1994).

For this study, the conceptual framework (see **Figure 3.1**) considers the challenges of cybersecurity governance as mentioned in (Swinton, 2019), (Ibid). It explores five primary challenges: cybersecurity strategy with business alignment, leadership commitment, standardized processes, enforcement and accountability, and resource allocation. It aligns these challenges with specific research questions to investigate and propose a comprehensive cybersecurity governance framework for ENIDP.

(ENISA, 2017) has defined cybersecurity culture as "the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest in people's behavior with information technologies. It is about making information security considerations an integral part of an employee's job, habits, and conduct, embedding them in their day-to-day actions." Most data breaches within organizations are caused by human actors (Micro, 2012), and while cybersecurity policies are common among organizations, employees may take it as guidelines rather than rules. In light of this, the creation of a cybersecurity culture accomplishes mindset change, promotes security awareness and risk perception, and upholds a close organizational culture instead of attempting to enforce secure behavior (Fagerström, 2013). On the other hand, corporate governance is the collection of duties that must be carried out by an organization's higher-level management structures, such as the management team, board of directors, and board and management committees (Mani, 2019). The board of directors of a company is responsible for overseeing the business's risk management efforts, which have to include cyber risk management as a key component (Broadman, 2018).

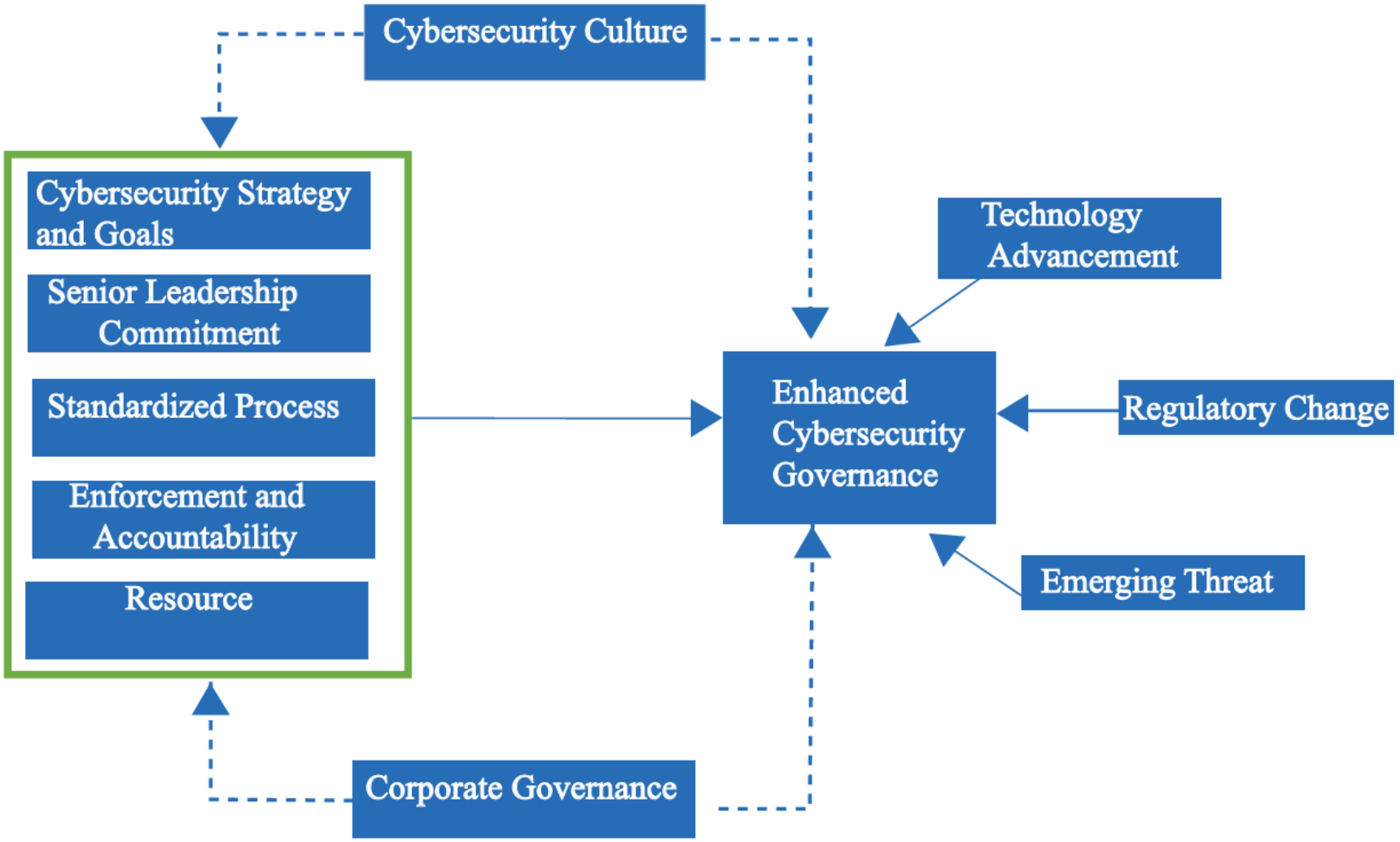

Figure 3-1 Conceptual Framework of the Study

A well-defined cybersecurity strategy that aligns with the business objective**,** supported by standardized processes, robust enforcement mechanisms, strong leadership commitment, and adequate resource allocation, plays a critical role in enhancing cybersecurity governance. These independent variables work together to create a comprehensive approach to managing cybersecurity risks and ensuring effective cybersecurity governance. Additionally, the presence of a well-established cybersecurity culture and sound corporate governance within an organization serves as confounding factors, influencing both the independent and dependent variables. These factors contribute to a more resilient and proactive cybersecurity posture, ultimately strengthening governance outcomes.

A strong cybersecurity culture leads to reduced risks of cyberattacks, enhanced data protection, and improved compliance with regulations. It fosters a proactive mindset among employees, encouraging vigilance and responsible behavior in handling digital assets. This culture not only minimizes security breaches but also ensures the organization is better equipped to respond to evolving threats, ultimately safeguarding its reputation, financial stability, and the confidentiality, integrity, and availability of critical information (Fonceca, April 2023).

Emerging threats, regulatory changes, and shifts in the technology landscape are external factors that significantly influence the effectiveness of cybersecurity governance within an organization. As new cyber threats arise, organizations must adapt their cybersecurity strategies, processes, and resource allocation to address evolving risks, which also puts pressure on leadership to remain proactive. Similarly, frequent regulatory changes demand updates to standardized processes and enforcement mechanisms**,** requiring agile adaptation to avoid compliance penalties and governance failures. The rapid pace of technological advancements, such as cloud computing and IoT, introduces new vulnerabilities that require constant adjustments in security strategies, as well as additional resources and training. In this context, a strong cybersecurity culture becomes essential for maintaining vigilance and effective security practices across the organization. These control variables emerging threats, regulatory changes, and technological shifts demand continuous monitoring, leadership commitment, and strategic adaptability, ultimately showcasing the dynamic nature of cybersecurity governance.

3.2. Research Design

In the methodological design, an inductive research approach was used. In making use of the inductive research approach, according to (Soiferman, April 2010) the researcher begins with specific observations and measures and then moves to detect themes and patterns in the data. The results of the exploration may later lead to general conclusions or theories.

3.3. Population and Sampling Design

3.3.1. Population

The target population of this study was employees of ENIDP.

3.3.2. Sampling Techniques and Sizes

Sampling is a process that enables information to be collected from a small number of individuals or organizations within a project or program, which can then be used to conclude a wider population (McCombes, 2019). There are many different sampling methods. Qualitative analysis typically relies more on smaller, purposefully chosen samples. The samples for this research were taken from the employees of the ENIDP, and the sampling technique employed was a type of non-probability sampling called purposive sampling. Employees with extensive knowledge of the program's operations and the ability to provide valuable insights into the issue were deliberately selected as respondethannts. At the time of the research, the ENIDP had a relatively small workforce, around less than 50 employees. Among them, 5 main respondents (this is based on the number of employees working in the cybersecurity area, they are not more than 15) were recruited purposively. Those at the management level (strategic-tactical levels) and working as experts in cybersecurity, technology, and legal areas were selected as respondents for the study.

3.4. Key Informants

In qualitative research, key informants are those who possess specialized knowledge, experience, or perspectives relevant to the research topic. They play a pivotal role in providing in-depth insights and understanding of the phenomenon under investigation. Key informants are typically selected based on their expertise, involvement, or relevance to the research context. According to Lincoln and Guba's seminal work on qualitative research methods (Lincoln, 1985), key informants

are essential for providing insider perspectives and deep insights into the phenomenon under study. By engaging with individuals who possess specialized knowledge or firsthand experience, researchers can enhance the credibility and richness of their qualitative findings. Additionally, the importance of selecting key informants strategically to ensure diverse perspectives and comprehensive understanding of the research topic is empahasazed by (Morse, 1991).

For this research, two key informants were purposively selected based on the hierarchical positions they held, their involvement in and understanding of the overall business activities of the ENIDP.

3.5. Data Sources

Both primary and secondary data were utilized in this research. The primary data were collected from respondents within the ENIDP office. In-depth interviews were conducted with individuals at both top-level and middle-level management to gather comprehensive insights. The secondary data were sourced from official ENIDP publications related to its mandate and gathered through document analysis techniques. The policies, legal and regulatory frameworks, and other documents released by ENIDP were considered for this research.

3.6. Data Collection Methods

The various data collection methods are discussed in detail below. The primary methods used for data collection were semi-structured in-depth interviews and document analysis.

3.6.1. In-depth Interview

An interview is an important qualitative research method in which the researcher collects data directly from the participants. When it is paired with other research methods like document analysis, interviews will be significant in unfolding opinions, experiences, values, and various other aspects of the population under study. Interviews are always goal-oriented. The type of interview this research has adopted was an in-depth interview. In-depth interviews are mostly long-duration, face-to-face, interviews conducted to achieve desired goals. The two suggestions for conducting in-depth interviews are the ‘Miner Metaphor’ and the ‘Traveler Metaphor’ (Showkat, July 2017). What the miner metaphor means is that knowledge is like a buried metal and it is the interviewer who unearths it. So far as the traveler metaphor is concerned, it means the interviewer

is a traveler who travels with the interviewee to get what he/she is after. In this method, both metaphors were followed for getting what the researcher was after.

3.6.2. Document Analysis

Document analysis is a systematic procedure for reviewing or evaluating documents both printed and electronic (computer-based and Internet-transmitted) material (Bowen, 2009). These documents can be advertisements; agendas, attendance registers, and minutes of meetings; manuals; background papers; books and brochures; diaries and journals; event programs (i.e., printed outlines); letters and memoranda; maps and charts; newspapers (clippings/articles); press releases; program proposals, application forms, and summaries; radio and television program scripts; organizational or institutional reports; survey data; and various public records. Scrapbooks and photo albums can also furnish documentary material for research purposes. These types of documents are found in libraries, newspaper archives, historical society offices, and organizational or institutional files. So, for this research, various ENIDP legal and regulatory frameworks related to the National Identification Program, as well as the country's cybersecurity and ICT policies, were considered.

3.7. Data Analysis

After collecting accurate and reliable data successfully by using the appropriate method from the source, the next step is how to extract the pertinent and useful information buried in the data for further manipulation and interpretation. The process of performing certain calculations and evaluations to extract relevant information from data is called data analysis (Ibrahim, January 2015). The data analysis may take several steps to reach certain conclusions. Simple data can be organized easily, while complex data requires proper processing. For this study, a qualitative thematic analysis method was used. Thematic analysis is a qualitative data analysis method used to identify, analyze, and report patterns (themes) within data (Clark, 2006). It is commonly used in disciplines such as psychology, sociology, education, and healthcare to gain insights into individuals' experiences, perceptions, and behaviors. Thematic analysis involves systematically coding and categorizing data to identify recurring themes, which are then interpreted to understand the underlying meaning or significance.

Steps in Thematic Analysis:

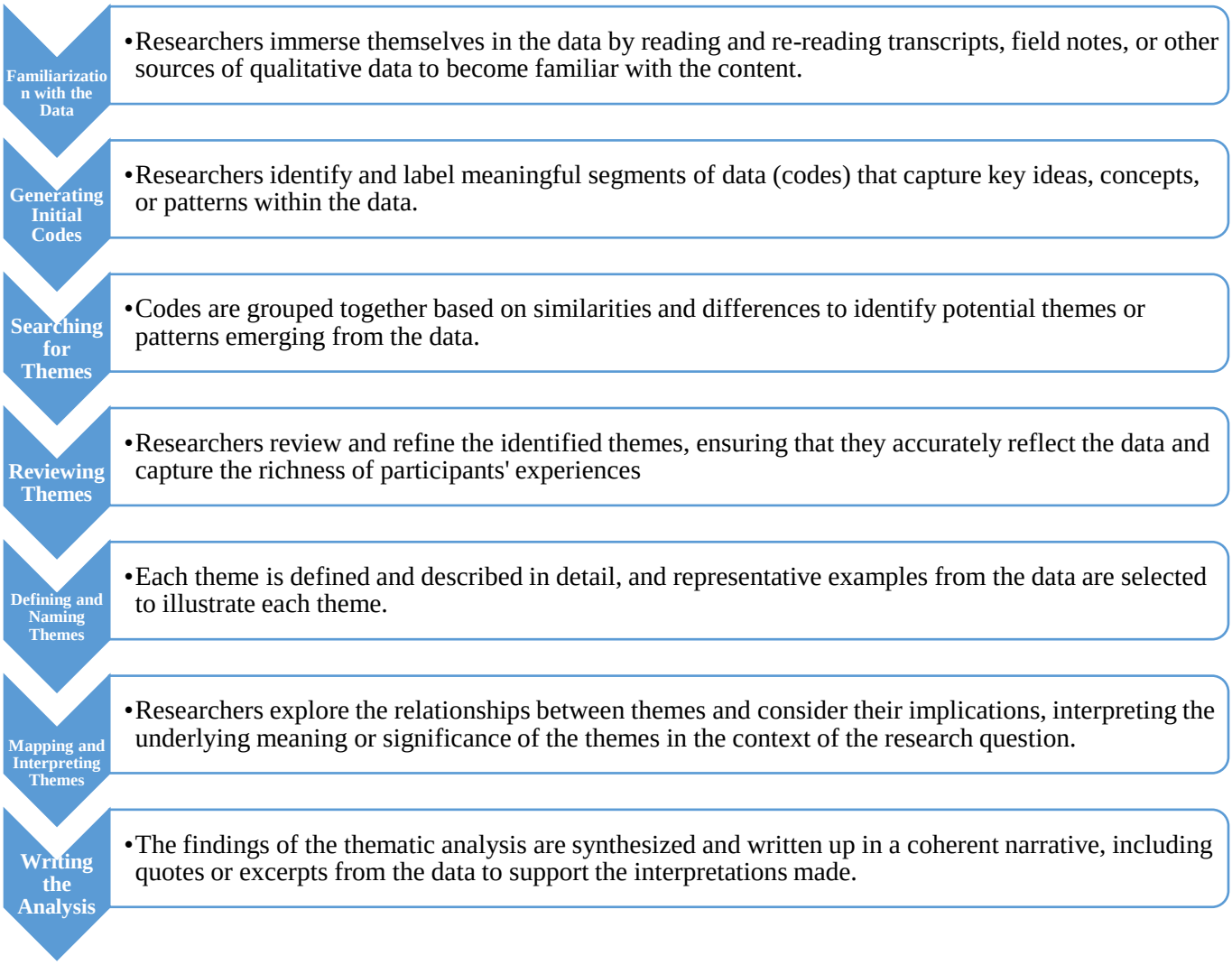

Figure 3-2: Thematic Analysis Process

These steps are supported by various scholars in the field of qualitative research, including (Braun, 2016), (Greg, 2012), (Lorelli, 2017), (Saldaña, 2015), and (Mojtaba, 2013). The basic works of these researchers and authors provide detailed insights into the theoretical underpinnings, practical applications, and methodological considerations of thematic analysis in qualitative research.

3.8. Ethical Consideration

The researcher made sure that the research design, methods, and data collection actions were ethical to ensure no harm or damage was caused. As ethics should be an integral part of every research, one way to achieve this is by asking at every stage of the research what is done is ethical (Thomas, 2017). Respondents were informed that taking part in the study is voluntary and a verbal

explanation of the study was given to the participants, and accordingly informed consent was obtained before collecting data (refer to **Appendix 1**). They were assured that their responses would be kept private and the data collected would never be used for purposes other than the research.

3.9. Framework Design Methodology

To design the framework, the researcher used a Design Science Research Methodology (DSRM). It is stated by (Jan, 2020) that DSRM is a problem-solving paradigm that seeks to enhance human knowledge via the creation of innovative artifacts. Simply put, DSRM seeks to enhance technology and science knowledge bases via the creation of innovative artifacts that solve problems and improve the environment in which they are instantiated. This methodology helps to successfully design science research by providing a generally accepted framework. Thus, the researcher used this methodology as it provides a structured process that is divided into phases.

Chapter Four: Data Analysis and Interpretation

4. Data Analysis and Interpretation of Results

To ensure the meaningfulness, understandability, and appropriateness of derived data, this stage involves thorough analysis. (Benjamin, 2017) distinguish qualitative data from quantitative data, emphasizing its diverse sources such as words, images, or documents. This research has adopted thematic data analysis techniques primarily, leveraging its theoretical flexibility and distinction from other qualitative approaches (Virginia, 2006).

Thematic analysis proves versatile, accommodating various research questions and diverse qualitative data types, including media, transcripts, focus groups, and interviews. In this research work, interviews were conducted by arranging suitable time frames for the respondents and being physically available where the interviewees were located, aiming for unbiased conversations devoid of emotional influence (Mandy, 2019). Subsequently, thematic data analysis was undertaken as the second step, followed by the extraction of key concepts derived from interviews (refer to **Table 4-1**) as the third and final step.

4.1. Qualitative Data Analysis Techniques

Qualitative data encompasses non-numeric information, including interview transcripts, notes, videos, audio recordings, images, texts, and documents. In this study, interview transcripts serve as the primary source of raw data. (Emma, 2018) delineate five categories of qualitative data analysis: content analysis, narrative analysis, discourse analysis, framework analysis, and grounded theory.

Thematic analysis was employed in this study to scrutinize interview responses, involving stages of familiarization, coding, category generation, theme review, theme definition and naming, and

final result write-up. This qualitative data analysis unfolds across three key steps. As outlined by (Bryman, 2007), the initial step involves code development and application. Transcripts are coded to categorize data, with codes representing themes or ideas. These codes progress through three categorization stages: open coding, wherein raw data is interpreted; axial coding, facilitating connections between code categories; and selective coding, constructing a coherent narrative by linking (ibid). The final output of the analysis is shown in **Table 4-1**.

4.2. Thematic Analysis

Table 4-1 below presents tabulated information generated from the thematic analysis of interview transcripts.

Table 4-1 Tabulatd Thematic Information

Themes	Category	Codes
Cybersecurity Strategy and Goal alignment with the Business Objective	Policy Development	NIS establishment, sensitive data protection, impending policy approval, alignment with strategy, experienced consultants, institutional level documentation, focus on critical assets, policy approval, ISO 27001 certification strategy, cybersecurity policy framework development
	Policy Implementation	Enacted policies addressing CS risks, continuous policy updates, effectiveness measurement, transition to policy implementation, challenges encountered, risk assessment outcomes
	Holistic Approach	People, Policies, Technology, ISMS, ISO 27001, policy implementation status, policies derived using the ISO 27001 ISMS risk-based approach, with four main processes identified: HR security, Identity Management, Asset Management, and Access Control, strong senior leadership commitment, governance structure, budget allocations, CS Directorate, integration of security measures, operational efficiency focus, expansion challenges

	Risk Assessment	Employee recruitment, cybersecurity training, risk identification, ISO Standard certification, top risk identification, data-focused ID system risks, policy and tool implementations
Senior Leadership Commitment	Team Structure	Cybersecurity team structure, team lead responsibilities, reporting line, division structure, team responsibilities, task communication flow, steering committee establishment, operational oversight, PMO guidance
	Commitment Basis	Business domain understanding, budget allocation, senior management support, policy discussions, external consultancy assignments, CS awareness training, implementation of ISO 27001 ISMS standards, incident reporting channels, hierarchical decision-making, critical incident handling procedures, policy development leadership, policy adherence monitoring, feedback review meetings
Standardized Process	Adherence to Standards	ISO standards, ISMS adoption, NIST Framework incorporation, implementation challenges, compliance objectives, gradual implementation approach, DevOps team establishment, MOSIP utilization, architecture suitability, unique ID generation
	Awareness and Feasibility	Organizational culture impact, employee awareness programs, cybersecurity training, cultural resistance, role-specific engagement, external consultant review, consent-based authentication, real-time verification mechanisms
Enforcement and Accountability	Legal Compliance	Data Protection Policy compliance, GDPR adherence, accountability under national laws, policy compliance, legal advisory influence, data privacy policy development, offense accountability, legal consequences, justice procedures, breach repercussions, alignment with legal requirements

Resource Allocation	Budget Allocation	Prioritization of cybersecurity, budget allocations, challenges with budget shortages, donor support, cybersecurity initiatives financing
	Human Resource Allocation	Budget constraints, top management understanding challenges, funding prioritization
	Budgetary Challenges	Tool purchase, cybersecurity training, policy implementation, audit allocation challenges
	Product and Service Viability	Product and service security balance, organizational needs prioritization, deadline prioritization, cybersecurity risk management, service delivery risk assessment
	Deadline vs Security	Deadline prioritization, cybersecurity risk management, service delivery risk assessment
	Cybersecurity Resource Allocation	Budget allocation, donor support, cybersecurity initiatives financing, cybersecurity challenge significance, resource scarcity impact
	Organizational Technology Structure	Engineering, Infrastructure, Cybersecurity, and Quality Assurance departments, team size comparison
	Resource Allocation Challenges	Cybersecurity challenge significance, resource scarcity impact
	External Support	Donor support overview, international organizations involvement, collective support benefits
	Governance Structure	Steering Committee establishment, operational oversight, PMO guidance
	System Architecture	Architecture Utilization, MOSIP utilization, architecture suitability, unique ID generation

4.3. Interview Transcriptions

According to (Kvale & Flick, 2009), data transcription is one of the most important steps before data analysis. In this study, the interviews were conducted by physically going to the offices of the respondents/participants. The derived interviews were recorded after obtaining the consent of all respondents. The first thing was visiting the respondents (principal respondents and key

informants) and arranging a timetable to conduct the interviews. Each interview lasted between approximately 40 minutes to 1:30 hours. Details regarding the participants and their employers in these interviews are hidden, as they are confidential and could lead to privacy concerns. As agreed in the consent form, which is part of the interview (see **Appendix 1**), the participants will remain anonymous, and assigned numbered pseudonyms (Respondent-1, Respondent-2, etc.). However, the office in which they are working and their positions are mentioned for the mere reason of asking specific questions about their status. This is one of the most important parts of this research, as it focuses on a new project Ethiopia is engaged in as one of its Digital Ethiopia-2025 initiatives.

Though there are no common rules about the transcription of interview data such as this, they must be correctly written, generated word to word, or only generated with primary answers following the questions asked (KvaleSteinar, 2007). Also, the researcher mentioned that transcription of interview data is a crucial step, as it needs to tackle several complex issues such as transmitting words from verbal to written form. Furthermore, (Meyer, 2001) noted that it authorizes the researcher's credibility to achieve a large amount of ease with every case which is capable of analysis and leads to the juxtaposing of the final results. In this transcription process, the respondents' responses were written in the Amharic language first. Second, the Amharic responses were translated into English in a word-for-word format. Finally, after the transcription of the interview data, the next step is data analysis.

4.4. Respondents

The selection of respondents is a critical phase in qualitative research and demands careful attention, as it profoundly influences the integrity of a study (Sarah, 2000). As (Patton, 2002) noted, qualitative inquiry deliberately delves deeply into relatively limited samples, sometimes even single cases. In this particular investigation, seven comprehensive semi-structured interviews were conducted. Amongst these, five of them were principal respondents working on the ENIDP under investigation that are top level and middle managements, and two of them were key informats who have participated in the management as well as in the various major activities related to ENIDP and they were selected based on their comprehensive knowledge of the overall activities under taken by the ENIDP which are external to the study area.

Interviews offer a flexible platform due to their semi-structured nature, providing ample room for nuanced responses to the research inquiries (Creswell, 2013). Before the final interview stage, a pilot test of the interview questions was conducted, ensuring clarity and comprehension among all participating respondents regarding each question's concept. Despite the relatively modest sample size, the interviews hold significant value as all respondents were seasoned professionals and executives, offering insightful perspectives on the internal workings of their respective corporations (David, 1998). Their candid contributions illuminate the intricate relationship between cybersecurity governance and ENIDP performance. Each interviewee was afforded ample time to articulate their insights. As the aforementioned authors suggested, it's worth noting that, the transcription process for a one-hour discussion can require 6 to 8 hours of work from an experienced transcriber, highlighting the labor-intensive nature of qualitative research compared to quantitative methods. The table depicted below shows the full details of the respondents who have assisted in this research willingly.

Table 4-2:Profile of respondents

Repondents	Gender	Position	Duation
Respondent-1	Male	CIO	42.01 Minutes
Respondent-2	Male	CEO	40:02 Minutes
Respondent-3	Female	Division Head (Legal Department)	31:05 Minutes
Respondent-4	Male	Director (Technology Head)	70:00 Minutes
Respondent-5	Male	CISO (Cybersecurity Division Head)	68.41 Minutes
KI-1	Male	Director and Deputy General Director	50:90 Minutes
KI-2	Male	Division Head (Cyber Law Division Head)	28:87 Minutes

Chapter Five: Discussion of Findings

5. Introduction

This study endeavors to explore the cybersecurity governance situation in the ENIDP. Purposive sampling was employed to select respondents from diverging departments within the ENIDP sector who are currently working at the management levels, ensuring that the sample comprises individuals capable of providing insightful perspectives on the various aspects of the sector. In addition to the interview, which is a pirmary source of data, document analysis was utilized to strengthen the data of the primary source to further enhance valuable insights to the research. A series of semi-structured interviews were conducted. While the sample size may be modest compared the staff working in the ENIDP, it is noteworthy that all interviewees hold high-level positions within the sector, bringing extensive experience and expertise to the discussions. Their candid insights into the operational dynamics of their organization provided invaluable insights into the extant cybersecurity governance situation within ENIDP. Each interviewee was afforded ample time to articulate their views, ensuring comprehensive coverage of the research topic.

In addition to the principal respondents selected through purposive sampling, this study also engaged key informants to enrich the research findings. These key informants, identified based on their in-depth knowledge and experience in relevant fields such as cybersecurity, cyber law, and cybersecurity governance & management, provided valuable insights and perspectives on the research topic. Their contributions complemented those of the principal respondents, offering additional context, nuances, and alternative viewpoints to enhance the depth and breadth of the study's analysis. Through targeted interactions and interviews with key informants, the research gained access to specialized expertise and insider perspectives that further elucidated the complexities of cybersecurity governance and its impact on cybersecurity within the ENIDP and similar contexts.

5.1. Findings of Results & Interpretation

1. **To what degree do the ENIDP's cybersecurity strategy and goals align with its business objectives?**

The primary research question investigates the interplay between ENIDP's cybersecurity strategy and goal and its alignment with its business objectives. Out of the thematic analysis we have done, the prominent answer we were able to discern was (1) the ENIDP's cybersecurity strategy emphasizes securing critical assets, including people, offices, technology, and data, which aligns with its business objectives of ensuring the integrity and security of identity-related information; and (2) policies and risk assessment processes are in place to address cybersecurity risks, indicating a proactive approach to aligning cybersecurity goals with business objectives. To further elaborate on this, one of the respondents said, "The ENIDP's business domain encompasses two main aspects: A) Registration, and B) Authentication, serving as the root of truth. These objectives are crucial for achieving our strategy and goals. Implementing these objectives is essential, as the data collected (biometric and demographic data) is inherently sensitive. Failure to protect this data could result in financial losses and hinder the achievement of our established objectives."

The response given by one of the respondents ensures that ENIDP is exerting its utmost effort to establish alignment between the cybersecurity strategy & goals and that of its business objectives. However, this is not confirmed by the key informants. For example, one of the key informants said, "*The national cybersecurity strategy and goals are established by INSA. INSA also drafts the National Cybersecurity Policy. It is the responsibility of all organizations to integrate the cybersecurity strategy and goals into their organizational structures. There is a comprehensive approach to the national cybersecurity system. However, regarding ENIDP, it is uncertain whether the cybersecurity strategy and goals have been established.*"

The National Science, Technology, and Innovation Policy (STI) Policy has incorporated various important direction that have many things to do with what the ENIDP is currently doing. The directions are infrastructure development that is pivotal to initiatives like the ENIDP, importance of a robust legislative framework to address issues of data privacy, security, and ethical considerations to ensure that the ENIDP operates within a framework that safeguards citizens' information and upholds public trust, advocating for rigorous monitoring and evaluation

mechanisms to ensure the accountability and effectiveness of initiatives like the ENIDP, and emphasizing on human resource development, particularly the cultivation of skilled manpower in fields such as science, engineering, and technology that is essential for driving the development and maintenance of the technological infrastructure that underpins the ENIDP and other STI initiatives.

Moreover, importantly, the STI Policy highlights the importance of international cooperation, recognizing the value of collaboration with global partners to bring expertise, resources, and best practices to initiatives like the ENIDP. By fostering international partnerships, Ethiopia can enhance the credibility and effectiveness of its ID program while also benefiting from knowledge exchange and capacity-building opportunities. In essence, the STI Policy serves as a comprehensive framework that not only supports the goals and objectives of the ENIDP but also contributes to Ethiopia's broader socio-economic development agenda through technological innovation and advancement (STI, October 2010).

What we can take from the principal respondents and the key informants is that binding policies are compelling each organization of the country to integrate cybersecurity strategy and goals within their organizational structures and business objectives, but those organizations are trying to meet these requirements albeit they haven’t put them to practice all in all. One thing we can be sure of is that the government of Ethiopia has been exerting its utmost efforts to enact information/cybersecurity/data protection policies and legal & regulator frameworks. What is lacking is the implementation of these frameworks. For instance, the National Information Security Policy was enacted in 2011, but now it is under revision for reasons like lack of implementation and not addressing dynamic and up-to-date cyber issues.

Despite the ambitious goals, the ENIDP project is behind schedule, with only 1.4 million people registered against the targets of 3 million by 2022, 6 million by 2023, and 70 million by 2025. Challenges include budget constraints and instability. The initiative aims to combat corruption and improve financial efficiency. Successful rollout requires prioritizing the project, addressing cybersecurity concerns, and possibly engaging major sectors in cost-sharing (Taye, 2023). Overall, the National ID Program has significant potential benefits but needs thorough planning and execution to succeed. This means that cybersecurity agendas are not dealt with to the required

degree and the cybersecurity strategy and goals are not fully aligned with the business of objectives of ENIDP.

2. **To what extent is senior leadership committed to providing strategic oversight and guidance for the organization's cybersecurity program?**

The second research question tried to cover whether there is any senior leadership commitment to provide oversight and direction in the already taken cybersecurity program. The overall response the respondents gave can be summarized as (1) senior leadership demonstrates a strong commitment to cybersecurity governance through budget allocations, establishment of a Cybersecurity Directorate, and quick problem resolution, indicating proactive oversight and guidance; and (2) the governance structure and resource allocations reflect a concerted effort by senior leadership to prioritize cybersecurity initiatives, ensuring adequate support and guidance.

To further elaborate on the summarized response, we can consider the response given by one of the respondents. The respondent said, "*There is a proposed organizational structure based on policy guidelines and ISO 27001 recommendations, with clearly defined roles for various personnel, including department heads responsible for the core cybersecurity team. Efforts are underway to implement these structures to the fullest extent possible. However, it's important to acknowledge the challenges involved in this implementation, particularly considering the country's practices, cultural norms, and organizational capabilities and inclinations. In some cases, security is perceived separately from governance, adding complexity to the process. Nevertheless, there is a strong commitment to the implementation process, starting from the executive level. While progress is underway, achieving full maturity in implementation remains an ongoing endeavor. Much of the decision-making process is currently centered around directors and managers, who are responsible for internal policies and procedures. However, the implementation of specialized procedures poses its own set of challenges, including the need for consistent attendance and availability."*

To confirm the responses given by the respondents, we can consider the response put forward in this case by one of the key informants. The key informant said, "*ENIDP has recently recruited a highly skilled cybersecurity professional team, notably establishing a dedicated cybersecurity department within its organizational structure. With the delineation of this structure comes clear roles and responsibilities for team members. The commitment to cybersecurity is evident through*

the formation of this specialized team. Under strong leadership, the team operates cohesively, with transparent communication and task visibility at all levels of the organization. This ensures thorough oversight of all activities. Moreover, the caliber of employees hired reflects a heightened level of professionalism, contributing to the overall efficacy of cybersecurity measures within ENIDP."

The National Information Security Policy of the Federal Democratic Republic of Ethiopia plays a crucial role in safeguarding sensitive data, including information collected and stored as part of the ENIDP. This policy establishes a comprehensive framework for managing information security risks, protecting against cyber threats, and ensuring the confidentiality, integrity, and availability of data. In the context of the ENIDP, which involves the collection and storage of vast amounts of personal and biometric information, the National Information Security Policy (NISP) provides essential guidelines and standards for securing this data against unauthorized access, breaches, and misuse (NISP, September 2011). The policy emphasizes risk management and compliance, aligning with the needs of the ENIDP, which faces security risks in handling sensitive personal data. It ensures legal adherence, crucial for safeguarding citizens' privacy rights and maintaining ethical data practices. By following this policy, the ENIDP can uphold data security, earning citizens' trust. Overall, the FDRE's NISP offers a robust framework for securing and managing data in organizations like ENIDP, mitigating risks, and preserving citizens' trust. All these important directions of the policy imply the commitment of the Ethiopian government in general and senior leadership of ENIDP in particular, in giving directions towards a safe and secure environment where the ENIDP flourishes within the country.

From the above discussions and the response given by one of the respondents and by one of the key informants, it can be said that there is a government and senior leadership commitment in oversighting the cybersecurity program within ENIDP. The Government of Ethiopia has legislated legal and regulatory frameworks and policies that are beneficial to bolster the security of the business activities within ENIDP. The senior leadership commitment in ENIDP is manifested through forming a cybersecurity division, onboarding employees with the required caliber, and proposing an organizational structure based on policy guidelines and ISO 27001 recommendations clearly defining roles for various personnel, including department heads responsible for the core cybersecurity team. Although the cybersecurity team was formed, ENIDP has government backing

in its endeavors, and it is trying to implement ISO 27001 throughout the ENIDP sector, the respondents indicated that there is a huge implementation challenges. This above finding and fact is also elaborated on a study (Melody Musoni, December 2023) that challenges to digital ID development in Ethiopia include updating regulatory frameworks, addressing uneven digital infrastructure, ensuring robust data protection, achieving financial sustainability, and bridging exclusion gaps among vulnerable populations. Collaboration between government, civil society, and international partners is crucial for developing tailored solutions suited to Ethiopia's needs. In a nutshell, there is government and senior leadership oversight concerning ENIDP, but the aforementioned challenges can be considered as bottlenecks to realize this ambitious plan of the country, especially the ones related to security and privacy issues.

3. **What are the most common challenges that ENIDP faces in implementing standardized processes for cybersecurity governance?**

The third research question addressed the various challegnes ENIDP came across in realizing standaridized process in relation to cybersecurity governance. The responses we were able to come up with from the thematic analysis we had conducted are recaputalated in put like (1) challenges in implementing standardized processes include employee resistance, incomplete understanding of systems, building a cybersecurity culture, and non-compliance due to internal behaviors; and (2) other challenges involve the simultaneous introduction of multiple systems, poor quality consultancy, and budget shortages, hindering effective implementation of cybersecurity governance processes.

Concerning these issues one of the respondents said, *"The implementation of ISO standards by INSA indicates an ongoing initiative within the ENIDP. However, challenges in complying with these standards stem from various factors, including the current working system, experience, culture, and mindset, all of which require significant change.* Change can be difficult; hence, it presents a challenge. *Transitioning to a new global organizational culture poses a substantial challenge. Adhering to standardized processes, particularly ISO 27001 compliance, is crucial for ensuring compliance and aligning with industry standards."*

On the fourth research question, one of the key informants said, "*It is important to adhere to standardized processes like ISO 27001 and highlighted that compliance should prioritize*

alignment with industry standards. Standardized processes encompass various aspects such as service, security, and customer handling. The primary challenge is building capacity, which requires significant investment in technology and time. Transitioning from compliance-driven to risk-based operations is a common obstacle. Personal experiences alongside standardized protocols can enhance outcomes. Engaging with departmental stakeholders is emphasized for assessing the efficacy of standardized processes and the interconnectedness of security efforts with the broader business objectives."

The paper by (Alqatawna, 2014) discussed the challenges of implementing information security standards in small and medium e-business enterprises (e-SMEs). It highlights the importance of security standards in evaluating and managing security, focusing on three major standards: Common Criteria, Systems Security Engineering-Capability and Maturity Model, and ISO/IEC 27001. Challenges such as cost, time consumption, and complexity are identified for each standard. While these standards provide frameworks for evaluating security, they may not fully address the needs of e-SMEs, especially in developing countries. The paper suggested potential modifications to these standards to better suit the e-SME context and emphasized the importance of a holistic approach to security. It is also discussed by (ISECUREDATA, 2023) the challenges of ISO 27001 that small businesses face when implementing ISO 27001, such as time, lack of expertise, limited budget, compliance maintenance, and integration with other standards. The site emphasizes the importance of seeking the guidance of an ISO 27001 consultant to overcome these challenges and ensure successful implementation.

The takeaway from the above two responses is that ENIDP is trying to implement ISO 27001 throughout its directorates and divisions alike. Yet, it came across various challenges that need to be resolved for the framework to be realized to its fullest extent. Some of the challenges can be cost, time limitation, complexity of the framework itself, and difficulty in integrating ISO 27001 with other existing frameworks. Other factors that are considered to be challenges for implementing standardized processes are the current working system, lack of capacity to implement standardized processes, experience, culture, and mindset of employees.

4. **How are enforcement and accountability controls implemented to facilitate compliance with relevant legal and regulatory cybersecurity frameworks?**

The fourth research question attempted to address the enforcement and accountability of legal and regulatory frameworks within ENIDP. To this end, the summarized succinct responses that were generated out of the thematic analysis are, (1) compliance with legal and regulatory frameworks is ensured through adherence to national and international standards, including the INSA CS Policy, Personal Data Protection Proclamation, and Computer Crime Law; and (2) accountability mechanisms involve incorporating legal requirements into organizational policies, implementing controls accordingly, and aligning policies with legal frameworks through due diligence.

To make some clarification to the above response, one of the respondents said, "*Ethiopia's Digital ID Decree 1284, Article 19:1, mandates robust information management systems for securely housing subscriber data. Article 17 emphasizes data protection and security, specifically Sub-Article 12, which requires strong safeguards against electronic attacks and data loss, and Sub-Article 13, which mandates efficient organization and secure storage of personal data. These provisions form the foundation of cybersecurity regulations, with detailed administrative controls for implementation. Additionally, the recently approved Personal Data Protection Proclamation, awaiting parliamentary approval, marks a significant advancement, reflecting modern international practices in data protection, contrasting with older legal categories like family law and property law."*

To counter-check the aforementioned response, one of the key informats replied in this respect, "*Unlike many other nations with mandatory cybersecurity requirements and accountability measures, our country relies on the willingness of parties to comply, resulting in voluntary adherence to cybersecurity protocols. Critical Information Systems (CIS), including digital IDs in security and financial institutions, lack legal provisions for identification and protection, as well as requirements for cybersecurity documentation, information security standards, and risk assessments. While the ENIDP's legal framework mandates personal data protection, the broader absence of personal data protection laws delayed the Digital ID system's implementation. The Computer-Crime Proclamation No. 58 penalizes offenses like unauthorized data access, but there is no dedicated cybersecurity law or regulatory body to enforce compliance and accountability. Consequently, accountability is limited to criminal actions under general computer crime laws, as the Criminal Code does not punish negligence unless intentional, highlighting the urgent need for a robust legal framework to address these cybersecurity gaps.*"

To further strengthen the previous claims, the Ethiopian Digital Identification Proclamation (EDIP) No. 1284/2023 establishes a reliable Digital Identification System in Ethiopia to ensure residents' rights, enhance service delivery, and promote transparency and efficiency. It aims to create a technologically advanced, cross-sector foundational system to facilitate national development, economic transformation, and good governance. The proclamation emphasizes the need for a comprehensive legal framework to regulate the use of digital identification, define stakeholder relationships, and ensure data security. It underscores the importance of digital identification in promoting social, political, and economic development, ensuring peace and security, and strengthening the justice system (EDIP, 2023).

The Personal Data Protection Proclamation (PDPP) clearly puts the enforcement and accountability issues which should also needs to be abide by the ENIDP (PDPP, 2021). The proclamation clearly stipulated that enforcement in Ethiopia's National ID Program is ensured through various measures outlined in Chapter Six of the document. The Commission is empowered to issue enforcement orders specifying violations, remedies, and compliance timelines. These orders serve as directives for data controllers and processors to rectify any contraventions promptly. Failure to comply can lead to administrative fines, with considerations such as the nature of the violation and harm to data subjects informing the fine's magnitude. Additionally, criminal offenses may be invoked for serious breaches, leading to imprisonment or fines. The Commission also possesses the authority to demand information from relevant parties through written orders, facilitating thorough investigations.

Accountability mechanisms are equally robust within the ENIDP framework. Individuals have the right to lodge administrative complaints against decisions made by data controllers or processors. The Commission oversees the transparent adjudication of these complaints, ensuring a fair process. Furthermore, an independent Appeals Tribunal provides an avenue for individuals to appeal Commission decisions, ensuring a thorough and impartial review process. Overall, these enforcement and accountability measures uphold the integrity of ENIDP, safeguarding the rights of individuals and ensuring compliance with data protection standards.

Concerning legal and regulatory frameworks to regulate privacy and data protection, (Haile, 2023) expressed that Ethiopia does not have a single and comprehensive legal instrument regulating

privacy and data protection, including the obligations of data controllers and processors, as well as the rights of data subjects in general. However, the author stated that there are legal and regulator frameworks comprising privacy and data protection provisions including the Constitution, the Mass Media Proclamation, and the Civil Code, which establish fundamental principles; specific regulations like the Digital Identification Proclamation, Criminal Code, and Computer Crime Proclamation address digital identity, cybercrime, and criminal offenses related to data; sector-specific laws like the Telecommunications Consumer Rights Directive, Financial Consumer Protection Directive, and Electronic Transaction Proclamation outline rules for protecting consumer data in telecommunications and financial sectors; and various other regulations govern areas such as healthcare, taxation, electronic transactions, and capital markets, contributing to a comprehensive framework for privacy and data protection in Ethiopia. Yet, the author (ibid) mentioned that the privacy and data protection framework in Ethiopia has significant gaps due to the lack of overarching legislation and reliance on sector-specific regulations, leading to inconsistencies. Children's data protection is absent, and key rights such as erasure, data portability, and protection against automated decision-making are not addressed. There are no mandatory contracts for data processors, fragmented enforcement mechanisms, and no unified data breach notification requirement. While some rights are partially covered, they are not uniformly guaranteed, and penalties for non-compliance vary widely.

From the three responses above, what can be taken is the fact that there are various legal and regulatory frameworks put in place to protect the sensitive data of the citizens of the country. But, one thing for sure is that there is a huge gap in practicing these legal and regulatory frameworks (along with their shortcomings) and there is no clear requirement to abide by for the sake of compliance.

5. **What factor influences the decision of the allocation of resources for cybersecurity programs?**

The last research question tried to uncover the extent to which resources are allocated for cybersecurity programs and initiatives within ENIDP. The summarized responses that were extracted out of the thematic analysis are: (1) resource allocation for cybersecurity is influenced by convincing top-level management, justifying business requirements against urgency, and securing specific budget allocations, including funding from external sources like the World Bank;

and (2) challenges in resource allocation include budget shortages, lack of attention to cybersecurity, understanding the issue, and a shortage of qualified staff, which impact decision-making regarding resource allocation.

To consolidate the above finding one of the respondents said, "*In cybersecurity, significant challenges include meeting government Key Performance Indicators (KPIs) while preventing security gaps, all amid resource scarcity. Ensuring equitable resource distribution for complex system development and operational intricacies is difficult. Financial backing must be secured to support manpower and resources. Additionally, external support is often necessary to overcome operational hurdles and enhance capabilities.*"

To counter-check the response given by the above respondent, one of the key informants said, " *The other aspect (ENIDP) is closely associated with security and national integrity. There is a question regarding whether external funding should even be considered. If such a program is feasible, and if the government can fully finance it independently, it would grant us more control and influence. One risk associated with external funding is the potential erosion of sovereignty. If the government implements a policy that contradicts the interests of the donors, they may withdraw their funding. Therefore, if we're unprepared, it could severely hinder our operations. This is a valid concern, which is why it's preferable, if possible, to be self-reliant. As I mentioned earlier, this is one of the threats we face, as funding could be terminated abruptly at any moment."*

The Labour Management Procedure (LMP) enacted by the ENIDP outlines a robust framework for labor management within infrastructure projects in Ethiopia, offering principles and procedures that are likely relevant to the ENIDP (LPM, November 2023). It emphasizes alignment with national policies and international standards, ensuring compliance with labor laws and ethical practices. By addressing risks such as child labor, forced labor, and occupational hazards, it aims to safeguard workers' rights and well-being. Clear grievance mechanisms are established to address any issues promptly and confidentially. Being tailored to the ENIDP, this framework provides valuable guidance for managing labor effectively within its context. The procedure clearly shows the extent the which ENIDP handled its human resources effectively and efficiently.

From the above responses, resource allocation is scarce for this case as there are things to give firsthand priority, yet the budget allocated for cybersecurity programs and initiatives, but what is worrying is that most of the funds for the programs are generated from donors, like UNDP, World

Bank and the, which will significantly harm if these donors stash away their funds. This finding is reaffirmed in a conference held in Gambia entitled “Digital ID and Interoperability” by the United Nations Economic Commission for Africa (UNECA) (UNECA, 2023) that glaring challenges for ENIDP are low level of infrastructure, low digital literacy especially in the rural areas, aligning all government priorities and strategies to reduce effort duplication and high budget demand.

5.2. Discussion of Thematic Analysis Results

The ensuing discussion draws upon the identified themes derived from the data analysis, which serve as the foundation for this research. For further elaboration and specific details, refer to Table 4-1.

1. **Theme 1: Cybersecurity Strategy and Goal alignment with Business Objective**

The thematic analysis revealed that the ENIDP's cybersecurity strategy is closely aligned with its business objectives of ensuring the integrity and security of identity-related information. By emphasizing the protection of critical assets such as people, offices, technology, and data, the ENIDP aims to safeguard its core business functions. The presence of policies addressing cybersecurity risks and regular risk assessments indicates a proactive approach to aligning cybersecurity goals with overarching business objectives. This alignment ensures that cybersecurity efforts are directed towards protecting the ENIDP's core operations and maintaining trust among stakeholders.

2. **Theme 2: Senior Leadership Commitment**

The theme of senior leadership commitment highlights its fundamental role in the successful implementation and sustainability of cybersecurity measures. This theme mainly encompasses team structure and commitment basis (the essence of commitment) and of which various aspects are included such as technology choices, organizational structure, clear reporting lines, budget allocation, resource management, adherence to standards, and engagement in policy development, as identified through the respondents' feedback. The selection of MOSIP as the identity management platform reflects senior leadership's commitment to cybersecurity, emphasizing security by design to safeguard critical systems from potential threats. This choice underscores the importance of integrating security considerations into the foundational aspects of technology infrastructure. The establishment of a well-defined cybersecurity team and clear reporting lines

further exemplify senior leadership's commitment. The presence of a governance structure and resource allocations tailored to cybersecurity initiatives reflects proactive efforts by senior leadership to prioritize cybersecurity and provide necessary support and direction. Additionally, senior management's allocation of necessary budgets for the cybersecurity team signifies their understanding of financial needs and the strategic importance of cybersecurity in protecting organizational assets and ensuring regulatory compliance. Support for implementation and adherence to standards such as NIST and ISO 27001 underscores their dedication to maintaining high cybersecurity standards. Furthermore, senior leadership's active participation in policy development and approval processes ensures that policies are well-informed, practical, and effective. In general, getting such attention from top-level management for the initiatives of cybersecurity ensures maintaining a resilient cybersecurity posture.

3. Theme 3: Standardized Process

The findings show based on the responses given by the respondents that, in addition to adhering to a national standardized process, at the highest level ENIDP is trying its level best to implement ISO 27001, which is a standard for information security management systems (ISMS). And according to the respondents ENIDP's ultimate objective is to secure an ISO 27001 certification. However, the respondents indicated that they are faced with a plethora of challenges.

The thematic analysis highlights several common challenges faced by the ENIDP in implementing standardized processes for cybersecurity governance. These challenges include employee resistance to new processes, poor staffing, incomplete understanding of systems, lack of required capacity, transitioning from a compliance-based to a risk-based approach, and the need to build a cybersecurity culture within the organization. Additionally, the simultaneous introduction of multiple systems, poor quality consultancy, difficulty in building a cybersecurity culture, and budget shortages pose significant hurdles to effective implementation.

Overcoming these challenges requires concerted efforts to educate and train employees, improve communication channels, develop a tailored cybersecurity governance framework as ISO 27001 is resource intensive & complex for implementation, and secure adequate resources for cybersecurity initiatives.

4. Theme 4: Enforcement and Accountability

The respondents claim that ENIDP has put in place robust enforcement and accountability mechanisms in the form of, for instance, Personal Data Protection Proclamation (which is highly influenced by GDPR) and Ethiopia's Digital ID Decree to ensure compliance with legal and regulatory frameworks. By adhering to national and international standards and incorporating legal requirements into organizational policies, the ENIDP demonstrates a commitment to upholding cybersecurity regulations. Furthermore, the alignment of policies with legal frameworks through due diligence and the establishment of accountability measures underscores the organization's commitment to maintaining legal and regulatory compliance. In addition, the PDPP compels ENIDP to comply with the provisions therewith, as it will be held responsible for any breaches of those rules. The respondents claimed there was no non-compliance issue up until then. And there is a legal and policy team organized to oversee the compliance process.

On the other hand, what we can infer from the thematic analysis is that there is a problem on the side of the employees to strictly abide by these legal and regulatory frameworks. Because the program is at its infancy stage, the respondents claimed that they are trying to familiarize themeseleves witth the legal intruments and trying to create awareness on the importance strictly buying the provisions of these framewors.

As such, it can be said that based on the views epressed by the respondents there are national legal and regulatory enfocement and accountability mechanisms (including the ones enacted internally by ENIDP itself). These frameworks help to make the activities being carried out in the program smoothly and minizing grivances of citizens and residents, whilst still respecting their privacies. However, there are problems like not adopting international instruments of the area, being negligent of the employees in meticulously following the provisions and lack of awareness on the importance of enforcement and accountability of the legal documents.

5. Theme 5: Resource Allocation

From the thematic analysis, we can see that the respondents claimed that suitable resource is allocated for cybersecurity agendas. Albeit a large proportion of ENIDP's budget is secured from international organizations like the World Bank, an all-encompassing budget is allotted specifically for cybersecurity. The resource allocation for cybersecurity programs is influenced by various factors, as indicated by the thematic analysis. Convincing top-level management,

justifying business requirements against urgency, and securing specific budget allocations, including funding from external sources, are critical factors in resource allocation decisions.

However, the respondents admitted that ENIDP is faced with various challenges in line with resource allocation for cybersecurity purposes including budget shortages, lack of attention to cybersecurity issues, being dependent on external donors, and a shortage of qualified staff may hinder effective resource allocation. Addressing these challenges requires strategic planning, effective communication, and advocacy for cybersecurity investments to ensure adequate resources are allocated to safeguard the organization's digital assets.

To strike a balance between the pros and cons uncovered in the thematic analysis of resource allocation, ENIDP should strive to customize its cybersecurity governance framework as it helps to simplify things and minize budgets for the activities undertaken therein. Effectively and efficiently planning and implementing its activities in such a way that it is possible to minize budgeting. And try to create some kind of local income generation mechanisms via collaboration with various stakeholders.

In summary, the thematic analysis provides valuable insights into the alignment of the ENIDP's cybersecurity strategy with its business objectives, the commitment of senior leadership to cybersecurity oversight, common challenges in implementing standardized processes, enforcement and accountability mechanisms for legal and regulatory compliance, and factors influencing resource allocation for cybersecurity programs. These findings can inform strategic decision-making and guide efforts to enhance cybersecurity governance within the organization. Based on the thematic analysis results the conclusions and recommendations are presented.

5.3. Conclusions

The ENIDP faces alignment challenges in matching its cybersecurity strategy with business objectives, struggling with budget constraints, instability, and unclear cybersecurity goals. Despite having policy frameworks like the National Information Security Policy, gaps in implementation and failure to address evolving cyber threats reduce their effectiveness.

Project execution challenges also hinder progress, with delays caused by budget and cybersecurity concerns, highlighting the need for better planning. The complexity of implementation requires

coordination across departments, integrating technology, and aligning with program goals. A comprehensive approach is essential, involving not just technical solutions but fostering security awareness and compliance.

Stakeholder collaboration is crucial for tackling cybersecurity issues. Continuous improvement is also necessary, with regular risk assessments and policy updates to keep up with evolving threats. Public trust depends on ENIDP's efforts to ensure data security. Finally, legal compliance with data protection and cybersecurity laws is vital to mitigate risks and protect citizens' rights.

5.4. Recommendations

Implementing these recommendations will help ENIDP overcome challenges, strengthen cybersecurity governance, and protect identity-related information while aligning with national objectives.

Strengthening budget and resource allocation is critical, with a dedicated funding stream for cybersecurity initiatives ensuring consistent support. In addition, enhancing policy implementation through regular updates will ensure ENIDP's frameworks address evolving threats. Improved project execution requires a clear management plan with accountability and risk strategies, while interdepartmental coordination can be facilitated by a centralized body overseeing cybersecurity efforts across departments.

A holistic approach to cybersecurity should combine technical solutions, staff training, and a security-focused culture, supported by regular audits and drills. Stakeholder engagement is key, to building partnerships with government and industry experts for collaborative problem-solving. ENIDP must also commit to continuous improvement, regularly reviewing and updating its policies to keep pace with evolving cyber threats.

Public trust is vital, and transparency through open communication and awareness campaigns will foster confidence. Cybersecurity efforts must align with national goals, supporting digital transformation and economic development as outlined in Digital Ethiopia 2025. Legal compliance is essential, with regular audits and staff training on data protection laws and regulations.

To further strengthen cybersecurity, ENIDP should enhance employee training to promote a security-aware culture and improve governance structures by clarifying roles, ensuring accountability, and having the cybersecurity department report directly to the CEO. Addressing implementation challenges through targeted support and advocating for increased investment in cybersecurity will enhance ENIDP's ability to mitigate risks and protect critical assets for long-term success.

Chapter Six: The Proposed Cybersecurity Governance Framework

6. Introduction

This chapter outlines the development of the proposed framework designed to address the research gap which is derived from the study's conclusion and recommendation. The framework offers a structured and systematic approach to enhance security through cybersecurity governance, guided by a set of foundational principles that ensure its applicability and relevance. Likewise, to assess the framework's implementation effectiveness, we have defined specific key performance indicators (KPIs), which serve as measurable criteria to evaluate its performance in various contexts. Furthermore, it is validated through security incident case scenarios to illustrate the practical implementation of the framework and showcasing how it operates under typical conditions.

6.1. Explanation and Evaluation of the Placement of the Cybersecurity Unit

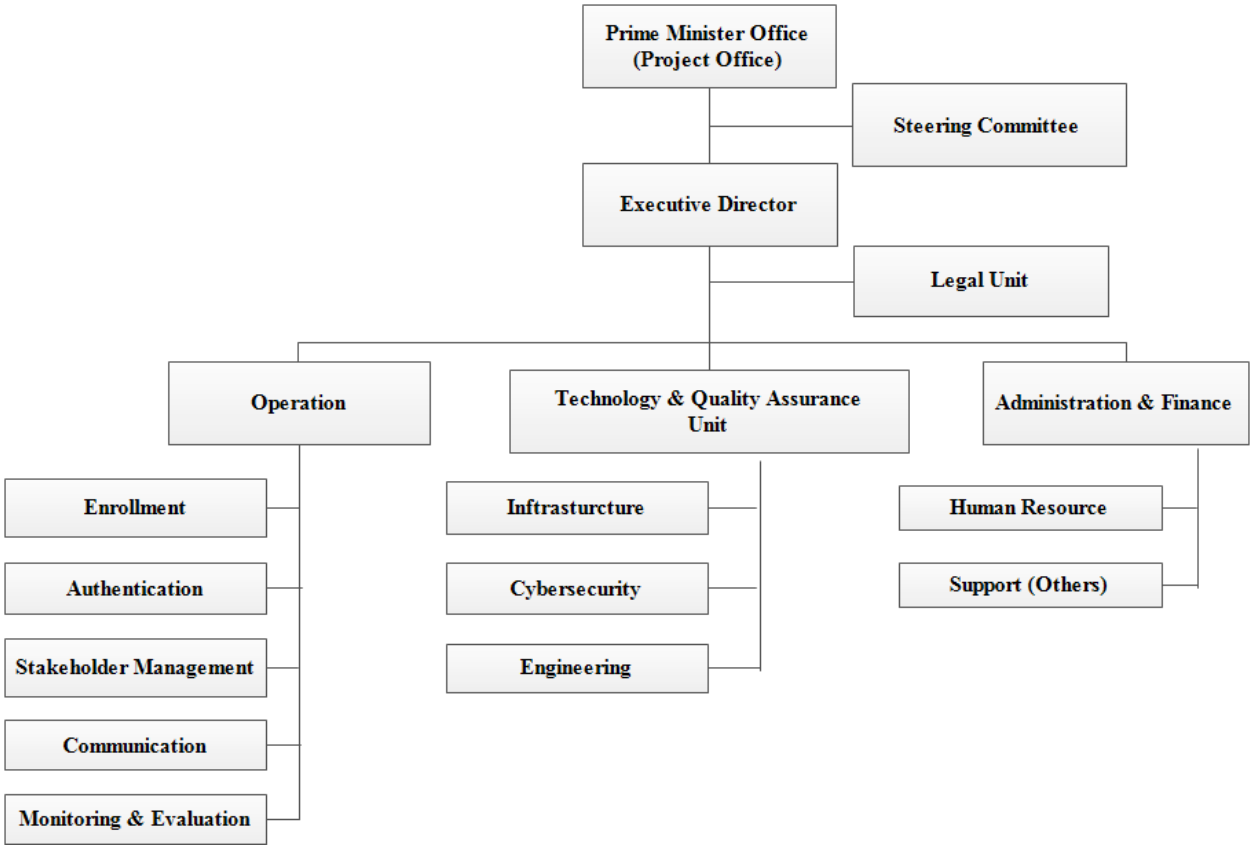

Figure 6-1: Organizational Structure of the ENIDP

The current organogram of ENIDP places the Cybersecurity Unit under the Technology & Quality Assurance Unit, highlighting the technically integrated nature. The placement allows the cybersecurity personnel to work closely with infrastructure and engineering functions for smooth operation and alignment with system development.

However, this organizational structure suffers from bad strategic visibility. Cybersecurity is not exclusively a technical or an exclusively governance and risk management issue. Its current location could inhibit its influence on executive decisions. Ideally, the unit should report to the Executive Director or be included under an independent Risk & Security Division in order to have necessary oversight and accountability.

From the above discussion, it is evident that the current place of the Cybersecurity Unit within the organizational setup is not ideal. Having it under the Technology & Quality Assurance Unit traps cybersecurity in a technical function alone, thereby reducing its strategic

visibility, powers, and interconnection with total organizational risk management and governance activities. This distribution does not reflect the high-priority need for cybersecurity to safeguard national digital identify infrasteructure, which must be addressed with an end-to-end holistic strategy encompassing policy, regulation, incident response, and interagency coordination.

Moreover, the absence of a clearly defined and tailored cybersecurity governance structure also heightens vulnerabilities to gaps in oversight, responsibility, and resilience. A proper cybersecurity governance architecture is required to connect cybersecurity objectives with those of national security, guarantee regulatory compliance, and ensure trust between stakeholders and citizens.

To address these limitations, we have developed a comprehensive Cybersecurity Governance Framework for the Ethiopian National ID Program. The framework provided in the next section is designed to enhance cybersecurity posture through improved organizational alignment, strategic direction, and operational effectiveness.

6.2. The Proposed Cybersecurity Governance Framework

The newly released NIST Cybersecurity Framework (CSF) V2.0 (February 2024) (Cherilyn Pascoe, 2024) helps organizations manage and reduce cybersecurity risks, regardless of their maturity or technical sophistication. Customizable, CSF 2.0 allows organizations to address specific risks and integrates cybersecurity with other enterprise risks, including financial, privacy, and supply chain risks. It provides clear, high-level outcomes for executives, managers, and practitioners, offering flexibility to map security controls effectively. It consists of three components: the CSF Core, which organizes cybersecurity outcomes into Functions, Categories, and Subcategories; Organizational Profiles, describing an organization's current or target cybersecurity posture; and CSF Tiers, measuring the rigor of cybersecurity.

Table 6-1 CSF 2.0 Core Function and Category Names and Identifiers

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

In this study, the researcher proposed a comprehensive Cybersecurity Governance Framework for the national identification program that aligned with the well-established NIST Cybersecurity Framework (CSF 2.0)**,** which is globally recognized as a best practice for cybersecurity management. The NIST CSF 2.0 outlines key functions; **Govern**, **Identify, Protect, Detect, Respond, and Recover (Table 6-1)** that are critical to managing cybersecurity risks (Cherilyn Pascoe, 2024). In the proposed framework, the functions are extended to incorporate governance elements (categories) and emphasize the role of leadership across the Strategic, Tactical, and Operational levels of an organization. This ensures beyond the technical aspects of cybersecurity

enabling the alignment of cybersecurity practices with organizational goals, culture, and strategic priorities.

In general, the proposed framework took three steps; firstly it redefined the NIST CSF Core Functions from a governance perspective, secondly, it introduced new categories under each function based on research findings **(Figure 6-3)**, and lastly, it aligned governance elements across leadership levels **(Figure 6-4).** Additionally **(Figure 6-5)** shows proposed component relationships as a compliment.

Adopting international cybersecurity standards can be challenging, often resulting in implementation gaps. The proposed framework addresses these gaps by clearly defining governance roles and responsibilities and ensuring accountability and transparency. The framework assigns cybersecurity governance responsibilities across leadership tiers; strategic, tactical, and operational **(Figure 6-4)**. While the NIST CSF V.2 offers governance in a broader sense, the research contribution provides a detailed allocation of duties at each different organizational level: such hierarchical assignment of governance roles offers a clearer, structured framework for integrating cybersecurity across leadership levels and strengthens the organizational accountability and ownership of cybersecurity practices. While it is designed for the national digital identity program, it can be adapted for other sectors by tailoring it to specific needs and integrating it with existing frameworks.

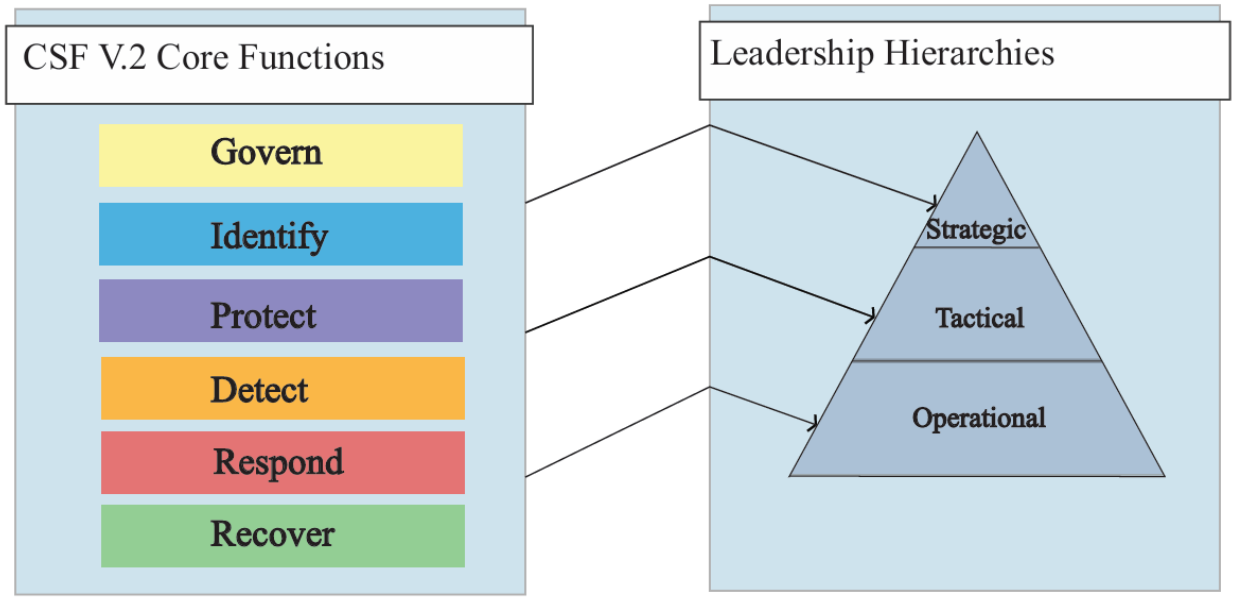

Figure 6-2 High-level Representation of the Proposed Cybersecurity Governance Framework

This comprehensive cybersecurity governance framework integrates strategic, tactical, and operational leadership roles with the NIST CSF 2.0 functions to enhance cybersecurity resilience for the ENIDP. It adopts a holistic approach to managing cybersecurity risks and aligns with organizational objectives. The following sections explore the definitions of NIST CSF 2.0 functions from a governance perspective, and the description of the proposed framwork.

Definitions of NIST CSF Functions from a Governance Perspective are given as follows.

1. **Govern**: Establish and maintain a comprehensive governance framework to direct, monitor, and control cybersecurity activities. This includes setting policies, defining roles and responsibilities, ensuring compliance with legal and regulatory requirements, and aligning cybersecurity initiatives with strategic objectives. Governance ensures accountability, oversight, and effective resource allocation for managing cybersecurity risks.
2. **Identify**: Develop a thorough understanding and management of cybersecurity risks to the organization's systems, assets, data, and capabilities. This foundational activity provides the necessary insights for informed decision-making and strategic planning.
3. **Protect**: Implement strategic safeguards to ensure the resilience of critical infrastructure and mitigate the impact of potential cybersecurity events. This function encompasses risk

mitigation strategies, legal and regulatory compliance, policy development and implementation, awareness and training, stakeholder engagement, technology integration, and fostering a cybersecurity culture.

4. **Detect**: Establish and maintain the capability to promptly identify cybersecurity events. This function focuses on implementing processes and technologies to continuously monitor and detect anomalies and potential threats, enabling swift and effective responses. It ensures a proactive approach to identifying cybersecurity incidents.
5. **Respond**: Develop and implement processes to effectively address detected cybersecurity incidents. This function ensures the organization is prepared to manage and mitigate the impact of cybersecurity events through coordinated actions.
6. **Recover**: Develop and implement incident recovery plans and procedures to restore and maintain operations following a cybersecurity incident.

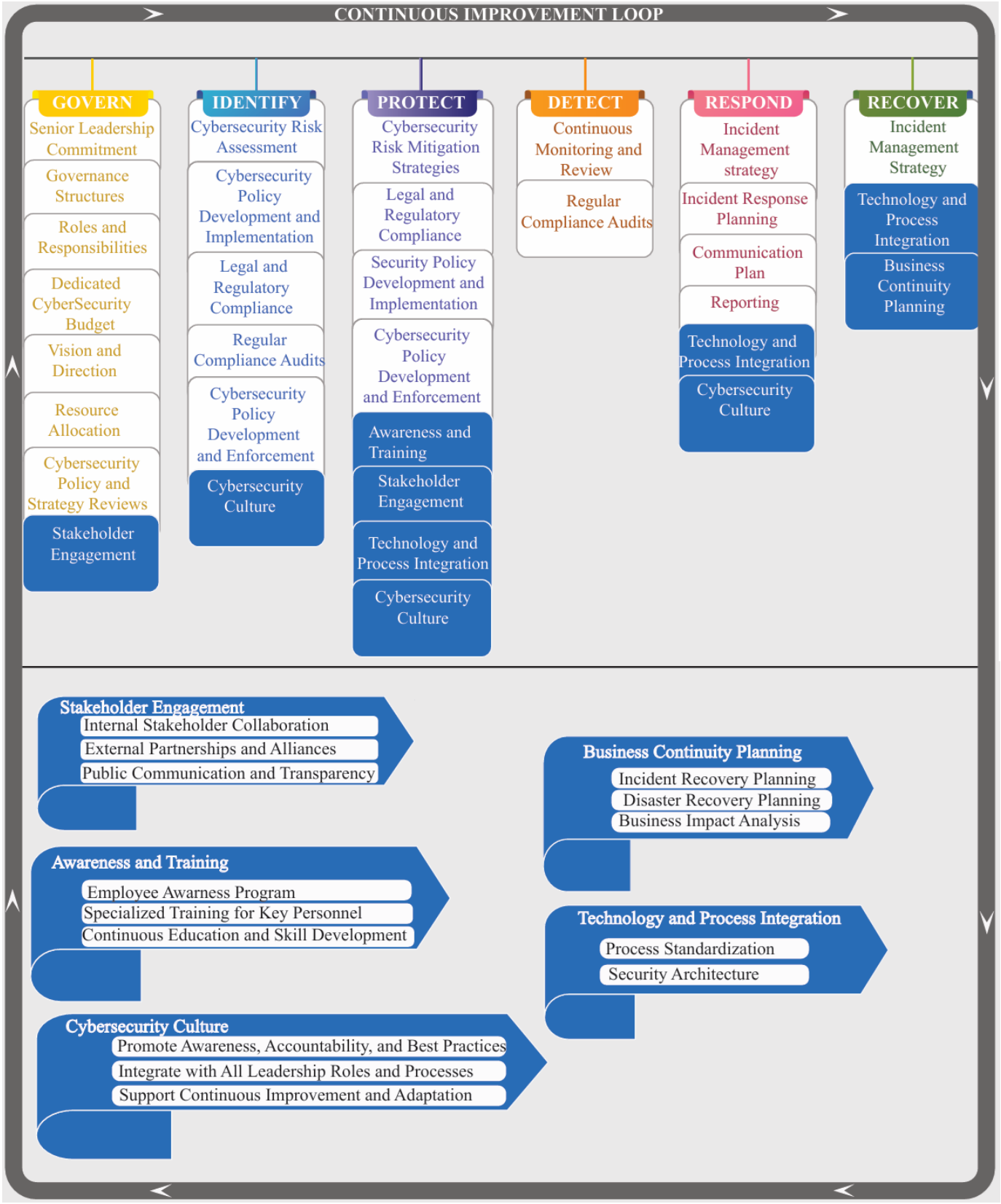

Figure 6-3 NIST CSF 2.0 Functions with Proposed Cybersecurity Governance Categories

Legend:

In Figure 6-3, (NIST CSF 2.0 Functions with Proposed Cybersecurity Governance Categories), categories highlighted in blue at the end of each function indicate the presence of subcategories. For example, within the “Recover” function, the “Business Continuity Planning” category is shown in blue, signifying that it has detailed subcategories, including “Incident Recovery Planning,” “Disaster Recovery Planning,” and “Business Impact Analysis.” These subcategories are displayed at the bottom of the image, separated by a line.

Figure 6-4 The Proposed Cybersecurity Governance Framework

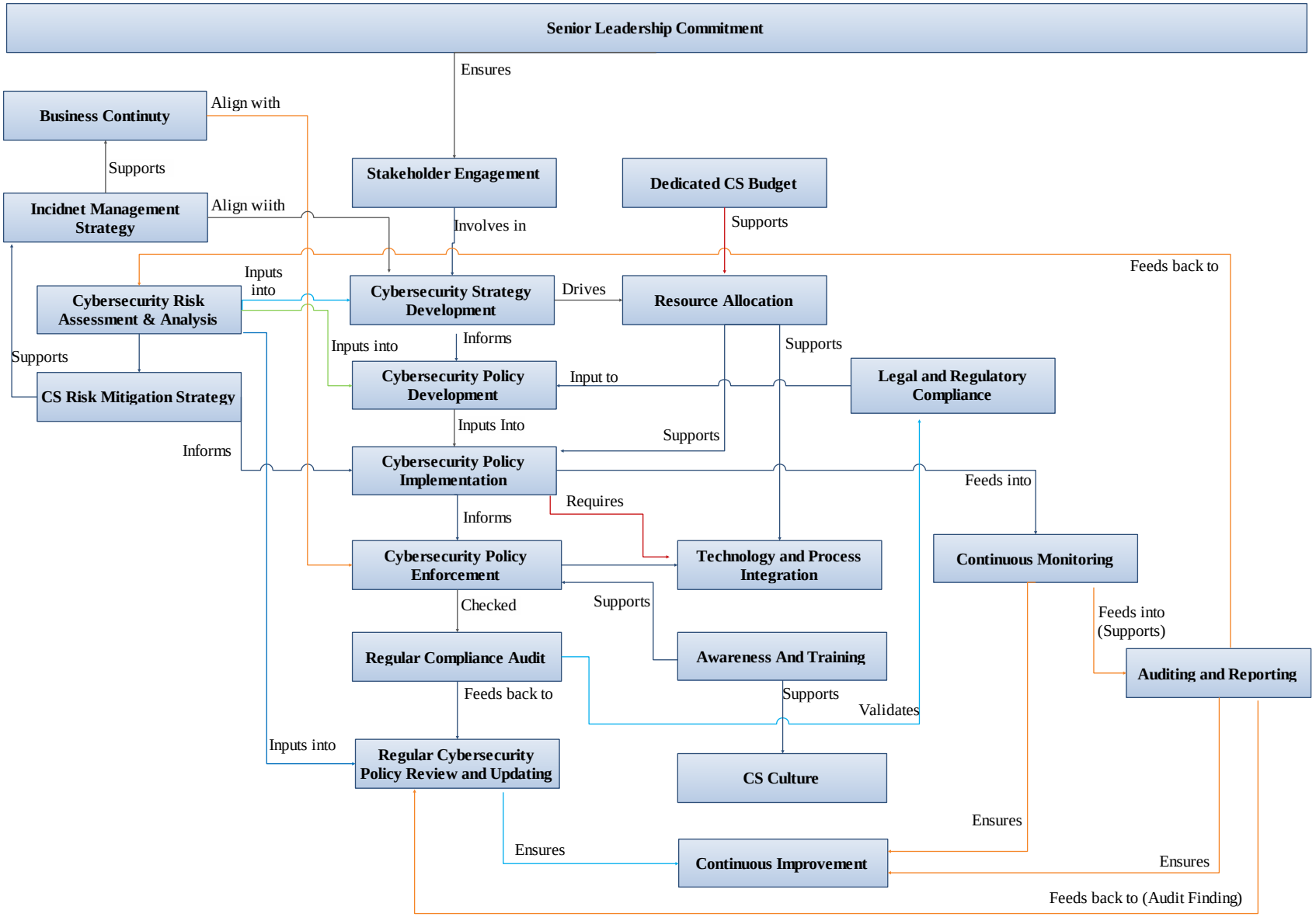

Figure 6-5 The Proposed Cybersecurity Governance Framework's Componenet Relationships

The following is the description of the proposed cybersecurity governance framework:
(Definitions of leadership levels integrated with the new categories functions) is stated below.

1. **Strategic Leadership**

- **Definition**: Strategic leadership involves setting long-term goals, defining the vision, and establishing the direction for the organization. It focuses on high-level planning and decision-making that aligns with the overall mission and objectives of the organization.
- **Importance**:
    - Provides a clear vision and direction for cybersecurity initiatives, ensuring alignment with organizational goals.
    - Ensures adequate resources, including budget and personnel, are allocated to cybersecurity efforts.
    - Demonstrates senior leadership's commitment to cybersecurity, fostering a security-first culture.
- **Roles**: Board of Directors, CEO
- **Responsibilities**:
    - **Senior Leadership Commitment (Govern)**: Ensure top management prioritizes cybersecurity, setting the tone at the top. There is demonstrated support for and active participation in cybersecurity activities, including resource allocation, risk acceptance, and accountability. This ensures cybersecurity is a strategic priority and that necessary resources are provided.
    - **Governance Structures (Govern)**: Establish clear governance frameworks, with defined reporting lines and decision-making processes.
    - **Roles and Responsibilities (Govern)**: Define the specific duties and obligations of individuals or teams involved in cybersecurity governance, while clarifying roles across departments to ensure accountability.
    - **Dedicated Cybersecurity Budget (Govern)**: Allocate a specific budget for cybersecurity initiatives.
    - **Vision and Direction**: Set the long-term vision and strategic goals for cybersecurity.

- **Resource Allocation**: Ensure adequate resources (budget, personnel, technology) for cybersecurity.
- **Cybersecurity Policy and Strategy Review (Govern)**: Periodically review and update Cybersecurity policies and strategies to ensure their effectiveness and alignment with organizational goals.
- **Cybersecurity Culture (Govern)**: Promote a culture of cybersecurity awareness and responsibility.

2. Tactical Leadership

- **Definition**: Tactical leadership focuses on translating the strategic vision into specific, actionable plans. It manages intermediate-term goals and develops processes and procedures to achieve strategic objectives.
- **Importance**:
  - Identifies and evaluates cybersecurity risks and develops mitigation strategies.
  - Develop cybersecurity policies and procedures and ensure effective implementation.
  - Continuously monitors and assesses cybersecurity measures to adapt and improve them.
- **Roles**: CISO, C-Suites, Risk Managers, IT Managers, Security Managers
- **Responsibilities**:
  - **Cybersecurity Risk Assessment (Identify)**: Regularly identify and evaluate cybersecurity risks.
  - **Risk Mitigation Strategies (Protect)**: Develop and implement strategic mitigation plans to mitigate potential cybersecurity risks.
  - **Continuous Monitoring and Review (Detect)**: Conduct ongoing oversight and assessment of risk management practices.
  - **Cybersecurity Policy Development and Implementation (Identify/Protect):** Create detailed policies for managing cybersecurity risks and translate strategic cybersecurity policies into specific actionable plans
  - **Cybersecurity Culture (Identify)**: Foster a culture that supports cybersecurity best practices and awareness.

- **Incident Management Strategy (Respond)**: Develop an incident management strategy to respond to cybersecurity incidents, ensuring quick and effective action. The entire lifecycle of an incident, from detection to resolution and post-incident analysis. Oversee the execution of incident response plans, ensuring policy adherence, and driving continuous improvement.
- **Stakeholder Engagement:** Collaborate with internal and external stakeholders to address cybersecurity challenges as cybersecurity is a shared responsibility
- **Reporting (Respond)**: Communicate cybersecurity findings to relevant stakeholders, including management, boards, and regulators.

3. Operational Leadership

- **Definition**: Operational leadership deals with the day-to-day management and execution of cybersecurity policies and procedures. It ensures the effective implementation of tactical plans and maintains the organization's cybersecurity posture.
- **Importance**:
  - Enforces cybersecurity policies and ensures compliance with legal and regulatory requirements.
  - Conduct regular compliance audits to identify and address gaps in the cybersecurity framework.
  - Manages operational aspects of cybersecurity for consistent and efficient protection of organizational assets.
- **Roles**: Operational Security Officers, Compliance Officers, Policy Administrators, Department Heads.
- **Responsibilities**:
  - **Cybersecurity Policy Development and Enforcement (Identify/Protect)**: Craft detailed cybersecurity policies (participate in the policy preparation with tactical leadership) and mainly ensure their enforcement.
  - **Legal and Regulatory Compliance (Identify/Protect)**: Ensure adherence to all relevant laws, standards, and regulations.
  - **Regular Compliance Audits (Identify/Detect)**: Conduct periodic audits to identify compliance gaps.

- **Continuous Monitoring and Review (Detect)**: Establish and maintain processes for collecting, analyzing, and responding to security-relevant information continuously to ensure continuous surveillance of cybersecurity systems to detect potential threats.
- **Incident Response Planning (Respond):** Implement and manage protocols for responding to cybersecurity incidents. Ensure that incident response plans are developed, tested, and maintained.
- **Business Continuity Planning (BCP):** Ensure the development of a Business Continuity plan that can enable an organization to continue its critical functions and operations in the face of a cyberattack or other disruptive event. It involves identifying potential threats, assessing their impact, and developing strategies to mitigate, respond to, and recover from such incidents.
- **Incident Recovery Planning (Recover)** is a critical subset of Business Continuity Planning (BCP) that focuses on the immediate response and recovery actions following a specific incident, such as a cyberattack, data breach, or system failure.
- **Disaster Recovery Planning (Recover)** is a critical subset of Business Continuity Planning (BCP) that specifically focuses on the restoration of IT systems and data after a disruptive event.
- **Business Impact Analysis:** Conduct Business Impact Analysis (BIA) as part of Business Continuity Planning (BCP) to identify and assess the potential impact of disruptions to critical business functions, processes, and assets and understand the consequences of cyberattacks to the organizations and prioritize recovery efforts.
- **Communication Planning** (Respond) Establish clear communication protocols for internal and external stakeholders during and after an incident. This includes notifying affected parties, coordinating with regulatory bodies, and providing updates to senior management and the board or to strategic and tactical leadership level).
- **Reporting (Response)**: Communicate cybersecurity findings, Incidents, and security-related based on the governance structure)
- **Employee Awareness Programs (Protect)**: Develop and maintain programs to educate employees about cybersecurity best practices and policies.

- **Technology and Process Integration (Protect/Respond/Recover):** Incorporate cybersecurity technologies and processes into the organization's overall operations. This category ensures that security measures are implemented effectively and also harmonized with other business functions to enhance overall security posture and operational efficiency.

The proposed cybersecurity governance framework offers several key benefits as outlined below:

1. **Integrated Governance Framework**: This approach aligns cybersecurity practices with the organizational structure, ensuring accountability and clarity in roles. It improves organizational resilience by aligning initiatives with business objectives and risk management strategies.
2. **Role Clarity and Accountability**: By clearly defining responsibilities across strategic, tactical, and operational leadership levels, the framework reduces overlap and gaps in governance. This enhances accountability and establishes mechanisms for tracking progress and addressing issues efficiently.
3. **Improved Decision-Making**: Enhanced communication pathways and reporting structures facilitate timely and accurate information flow, allowing leaders to make informed, strategic decisions based on relevant context.
4. **Scalability and Flexibility**: The framework is adaptable for organizations of various sizes and industries, ensuring its relevance and effectiveness across diverse contexts.
5. **Performance Measurement and Continuous Improvement**: Integrating performance metrics and key performance indicators (KPIs) promotes ongoing monitoring and enhancement of cybersecurity policies, procedures, and controls through regular feedback loops.
6. **Promotion of a Security Culture**: By embedding cybersecurity practices in leadership roles, the framework fosters a culture of security awareness and responsibility among all employees, essential for protecting organizational assets.
7. **Compliance and Standardization**: The framework aids organizations in meeting regulatory requirements by incorporating standardized practices from the NIST CSF, ensuring adherence to legal standards while promoting industry best practices.

6.2.1. Principles for the Proposed Cybersecurity Governance Framework

The following principles should be adopted to enhance the effectiveness of the proposed cybersecurity governance framework for the ENIDP. To align with the core characteristics of a national identification system, the principles have been adopted from the World Bank's 10 global Identity for Development (ID4D) principles, which are recognized as the principles of identification for sustainable development in the digital age and others like ISO 27014, COBIT 2019, ENIDP-Principles, GDPR, and PDPP. These principles have been specifically tailored to Ethiopia's national ID program to ensure it adheres to global best practices.

Table 6-2: Principles for the proposed cybersecurity governance framework

Principle	Description	Principle Mapping
Transparency	Ensure clear communication and openness about cybersecurity policies, practices, and incidents.	• **ENIDP-Principles (Communications)**
Privacy	Protect individuals' personal data by implementing robust privacy measures.	• **ENIDP-Principles (Privacy and Minimal Data Collection)**
Data Minimization	Collect and retain only the minimum amount of personal data necessary for the ID program.	• **ENDP-Principles** (Privacy and Minimal Data Collection) • **GDPR**: Article 5(1)(c) (Data minimization)
Purpose Limitation	Use personal data solely for the purposes specified and communicated to data subjects.	• **PDPP: Article 13** • **GDPR**: Article 5(1)(b) (Specified purposes only)
Accountability	Ensure that all cybersecurity actions and decisions are accountable to senior leadership and stakeholders.	• **ID4D-Principle 9** (Establishing clear institutional mandates and accountability)
Integrity	Maintain the accuracy, consistency, and trustworthiness of data.	• **GDPR**: Article 5(1)(d) (Data integrity)

Security	Protect data and systems from unauthorized access, disclosure, alteration, and destruction.	• **ID4D-Principles** (Establishing a robust—unique, secure, and accurate—identity) • **ENIDP-principles** (Security in Design)
Resilience	Ensure the ID program can withstand and recover from cyber incidents.	• --
Ethical Use	Ensure the ethical use of data and technology in the ID program.	• --
Continuous Improvement	Continuously enhance cybersecurity practices to address evolving threats.	• **ITIL-Guiding-Principles (**Progress iteratively with feedback)
Holistic Approach	All the leaders across the business units (cybersecurity, legal, technology, and other business units) shall work harmoniously taking a shared responsibility in their cybersecurity governance role.	• **COBIT 2019 Principles**
Interoperability	Ensure cross-sector (government agencies, private sector, and relaying parties), and cross-border integration and communication	• **ID4D-Priciples** (Creating a platform that is interoperable and responsive to the needs of various users.)
Risk-based approach	Have ongoing monitoring and assessment to ensure that decision-making is risk-based and aligned with the organization's risk appetite; enabling targeted cybersecurity investments that avoid unnecessary spending on low-risk areas while reinforcing defenses where they are most needed.	• **ISO 27014:2020** Principles (Objective 2)

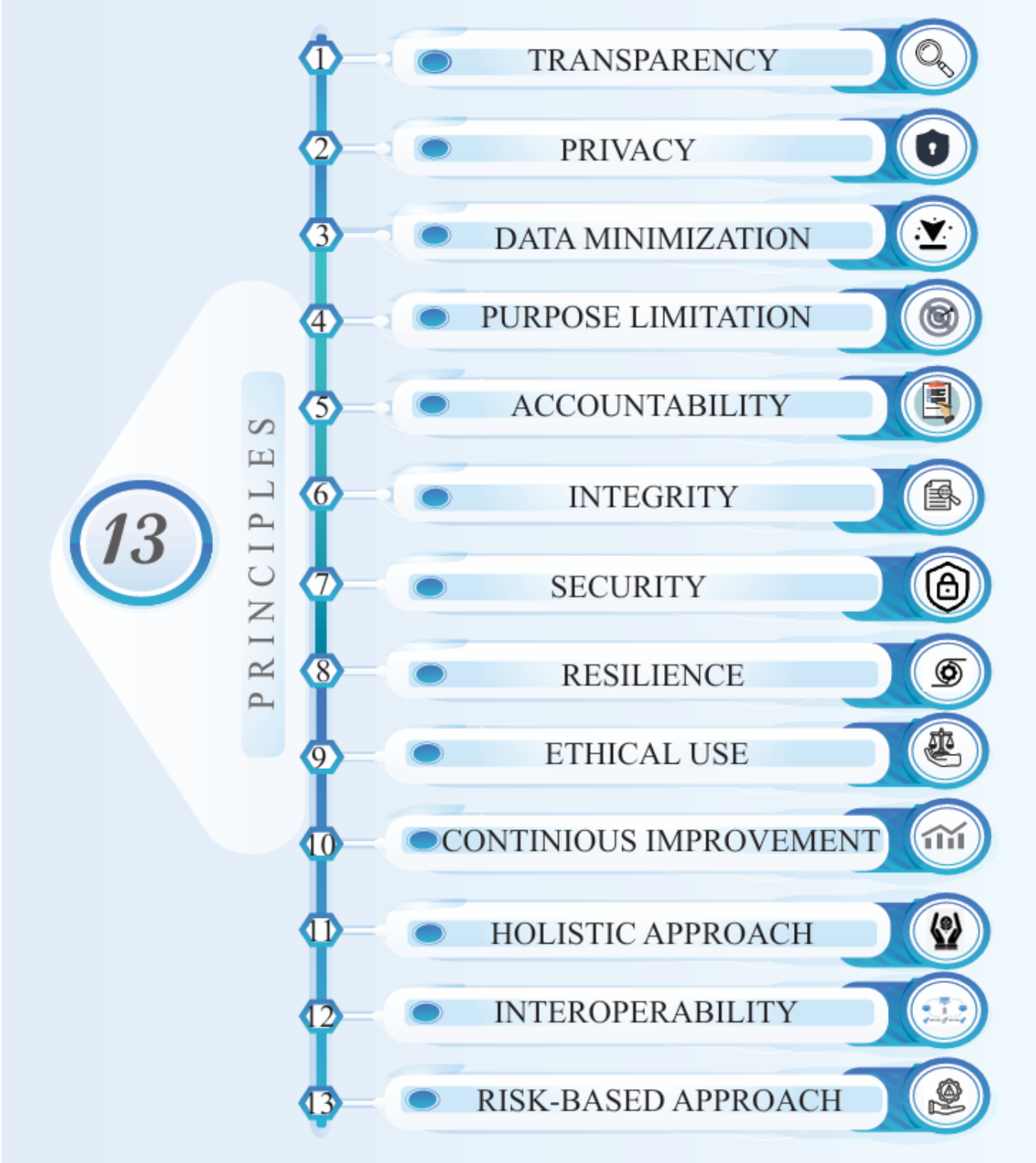

Figure 6-6 Guiding Principles for the cybersecurity Governance Framework

6.2.2. Key Performance Indicators for the Proposed Cybersecurity Governance Framework

To measure the effectiveness of the proposed cybersecurity governance framework for the ENIDP, it's crucial to establish Key Performance Indicators (KPIs) that align with the principles. These KPIs provide quantifiable metrics to monitor progress, identify areas for improvement, and ensure that cybersecurity objectives are met. These KPIs will help in monitoring the effectiveness of the cybersecurity governance framework in achieving the strategic objectives of the ENIDP.

Table 6-3 Key Performance Indicators for the Proposed Cybersecurity Governance Framework

Leadership Levels and Other Activities	Category	KPI	Expected Outcome
Strategic	Senior Leadership Commitment	Percentage of cybersecurity initiatives approved by senior leadership.	Increased alignment and prioritization of cybersecurity initiatives with business strategy, fostering a proactive security culture.
		Frequency of cybersecurity updates and reviews by the executive board.	Improved executive awareness and timely decision-making regarding evolving cybersecurity threats and risks.
	Governance Structures	Number of governance meetings held per quarter.	Stronger governance oversight, resulting in well-coordinated cybersecurity policies and practices.
		Attendance rate at governance meetings (Percentage of board and committee members attending	Enhanced leadership engagement and accountability in cybersecurity initiatives.

		cybersecurity meetings as required).	
		Compliance rate with established governance frameworks (Percentage of governance policies fully complied with across the organization).	Better policy enforcement, reducing risk exposure and increasing operational resilience.
	Vision and Direction	Alignment of cybersecurity strategy with business objectives.	Improved strategic alignment, ensuring cybersecurity supports overall business growth and resilience.
		Frequency of strategy reviews in response to emerging threats.	Greater agility and preparedness in adjusting to new and evolving cybersecurity threats.
	Dedicated Cybersecurity Budget	Percentage of overall IT budget allocated to cybersecurity.	Sufficient and effective resource allocation ensuring comprehensive protection against threats.
		Annual increase in cybersecurity investment aligned with threat landscape changes.	Enhanced risk mitigation and threat response capabilities, keeping pace with the evolving cyber landscape.
Roles and Responsibilities	Percentage of staff with clearly defined cybersecurity	Percentage of staff with clearly defined cybersecurity roles and responsibilities.	Clear cybersecurity role and responsibility and Accountability

	Roles and Responsibilities.	Time taken to assign roles and responsibilities after organizational changes.	Faster adaptation to organizational changes, ensuring no gaps in cybersecurity coverage.
		Percentage of employees or teams adhering to cybersecurity policies as part of their defined responsibilities.	Increased compliance with cybersecurity duties, reducing potential vulnerabilities due to human error.
Tactical	Risk Assessment	Number of risk assessments conducted annually.	Proactive risk identification, leading to a continuously updated risk landscape and improved defensive posture.
		Percentage of identified risks mitigated within a specified timeframe.	Effective and timely risk management, reducing the potential impact of security breaches.
	Policy Implementation	Number of new or updated cybersecurity policies implemented annually.	Updated policies that reflect the latest cybersecurity best practices, increasing organizational resilience.
		Compliance rate with internal cybersecurity policies.	Improved adherence to policies, resulting in reduced incidents and stronger compliance.
		Stakeholder feedback on policy effectiveness.	Stronger engagement and feedback loops that contribute to continuous improvement of cybersecurity measures.

Risk Mitigation Strategies	Implementation rate of risk mitigation plans.	Percentage of Risks with Mitigation Plans	Comprehensive mitigation strategies that reduce overall risk exposure.
		Implementation rate of risk mitigation plans.	Timely implementation of mitigation strategies, leading to reduced vulnerabilities and enhanced resilience.
		Reduction in the number of identified vulnerabilities year after year.	Decreased vulnerability count, resulting in enhanced network and system security.
Continuous Monitoring and Review	Average time to detect security incidents.	Average time to detect security incidents.	Faster detection of incidents, minimizing damage and response time.
		Number of successful detection events versus false positives.	More accurate detection, improving security team efficiency and focus on real threats.
		Number of Non-Compliance Issues Detected through Continuous Monitoring	Reduced regulatory penalties and increased adherence to industry standards.
		Percentage of Security Incidents Properly Documented and Reported	Improved incident reporting and analysis, fostering a culture of transparency and continuous improvement.
Operational	Cybersecurity Policy Enforcement	Number of enforcement actions taken against policy violations.	More consistent enforcement reduces policy breaches and strengthens overall compliance.

		Frequency of policy breaches due to non-compliance.	Fewer breaches due to stronger policy enforcement and employee adherence.
		Percentage of business processes adjusted to align with new/existing cybersecurity policies.	Streamlined integration of cybersecurity into business processes, improving operational security.
Legal and Regulatory Compliance	Number of compliance audits conducted annually.	Number of legal and regulatory compliance audits conducted annually.	Minimized legal penalties, fines, and reputational damage through proactive compliance.
		Compliance rate with relevant legal and regulatory standards.	Higher compliance rates, ensuring the organization operates within legal frameworks and reduces risks.
Regular Compliance Audits	Percentage of audit recommendations implemented within six months.	Percentage of audit recommendations implemented within a specified time.	Faster and more comprehensive audit compliance, ensuring regulatory adherence and risk minimization.
		Frequency of internal and external compliance audits.	Regular internal and external audits to ensure ongoing compliance.
Awareness and Training	Employee Awareness Programs	Percentage of employees who have completed cybersecurity awareness training.	Higher employee awareness reduces human error and strengthens the organization's security posture.

		Number of cybersecurity awareness campaigns conducted annually.	Continuous education promotes a culture of cybersecurity vigilance.
Specialized Training for Key Personnel	The number of specialized training sessions for key personnel.	Number of specialized training sessions for key personnel.	Enhanced skillsets among key personnel, improving incident response and specialized risk management.
		The number of role-based specialized training conducted.	Increased role-based specialized training sessions to enhance targeted skills.
		Certification rate among key cybersecurity personnel.	Increased certification rates, leading to higher expertise in managing advanced cyber threats.
Continuous Education and Skill Development	Frequency of continuous education programs.	Frequency of continuous education programs.	Regular delivery of continuous education programs to maintain skills and awareness.
		Employee satisfaction and proficiency levels post-training.	Improved employee satisfaction and proficiency following training.
Stakeholder Engagement	Internal Stakeholder Collaboration	Number of interdepartmental cybersecurity meetings.	Stronger internal collaboration, improving organizational-wide security practices.
		Rate of internal stakeholder participation in cybersecurity initiatives.	Higher engagement leads to more cohesive and integrated cybersecurity efforts.

External Partnerships and Alliances	The number of partnerships with external cybersecurity organizations.	The number of partnerships with external cybersecurity organizations.	Broadened expertise and resources through collaboration with external cybersecurity experts.
		Frequency of joint cybersecurity initiatives with external partners.	
		The number of formal cybersecurity-related meetings held with stakeholders over a specified period.	Increased formal cybersecurity meetings with stakeholders to enhance collaboration.
Public Communication and Transparency	Number of public communications related to cybersecurity.	Number of public communications related to cybersecurity.	Increased public communications about cybersecurity to enhance transparency.
		Public trust index (It is measured through surveys and feedback.)	Higher public trust, reflecting confidence in the organization's security and transparency practices.
Technology and Process Integration	Security Technology Implementation	Percentage of planned security technologies successfully implemented.	Advanced technology integration reduces security gaps and enhances threat prevention.
		Reduction in security incidents due to new technology deployments/ cybersecurity policy development or update.	Fewer security incidents due to stronger technological defenses.
Process Standardization	Standardization rate of cybersecurity processes.	Standardization rate of cybersecurity processes.	Higher standardization rate of cybersecurity processes for improved consistency.

		Efficiency improvements due to standardized processes.	Streamlined operations that enhance overall cybersecurity management.
Incident Response and Recovery	Average incident response time.	Average incident response time.	Reduced average incident response time for faster threat mitigation.
		Percentage of incidents successfully contained and recovered from.	Improved recovery rates, minimizing the impact of breaches on business operations.
Continuous Improvement	Regular Policy and Strategy Reviews	Frequency of policy and strategy review sessions.	Regular policy and strategy reviews to ensure alignment with evolving needs.
		Number of updates made to policies and strategies annually.	Increased annual updates to policies and strategies for continuous improvement.
		Cybersecurity strategy and Policy alignment with business.	Better alignment of cybersecurity strategy and policies with business objectives.
Adaptive Strategies to Evolving Threats	The number of adaptive measures implemented in response to new threats.	The number of adaptive measures implemented in response to new threats.	Increased adaptive measures in response to new threats for enhanced security.
		Reduction in the impact of new cybersecurity threats.	Decreased impact of new cybersecurity threats through effective mitigation.
Cybersecurity Culture Development	Cybersecurity Culture	The percentage of employees and relevant stakeholders who complete mandatory cybersecurity	High completion rate of mandatory cybersecurity

		awareness training within a specified period.	awareness training among employees and stakeholders.
		Reduction in cybersecurity incidents attributed to human error.	Decreased cybersecurity incidents due to reduced human error.
Resource Allocation	Resource Allocation	Percentage of resources allocated to high-risk areas identified in risk assessments.	Increased allocation of resources to high-risk areas identified in risk assessments.
		Adequacy of resource allocation relative to cybersecurity needs.	Sufficient resource allocation aligned with cybersecurity needs.

6.2.3. High-Level Proposed Framework Implementation Guide

The following illustration serves as a high-level guide for implementing the proposed Cybersecurity Governance framework. The framework, developed as part of the research, aims to provide a robust and systematic approach to managing cybersecurity risks and ensuring compliance with relevant regulations, and assist organizations in effectively adopting and implementing the framework. It covers the following key aspects:

1. Board and Leadership Involvement

- Develop a membership of the board of directors focused on cybersecurity oversight.
- Establish a cybersecurity steering committee composed of senior management executives including cybersecurity and legal business unit representatives.
- Engage the board in setting the organization's risk appetite and tolerance levels.

2. Cybersecurity Governance Structure

- Develop a cybersecurity governance structure with clear roles and responsibilities under each leadership hierarchy (strategic, tactical, and operational levels).
- Define the decision-making authority and escalation paths for cybersecurity issues.

3. Risk Management

- Perform organization-wide security risk assessments considering internal and external factors.
- Develop and periodically update a risk mitigation strategy based on assessment results.
- Allocate cybersecurity resources based on risk appetite, tolerance levels, and priority risks.

4. Strategic Direction and Policy Development

- Set cybersecurity strategic directions and develop a comprehensive cybersecurity strategy document.
- Develop security policies that cascade from the cybersecurity strategy and are informed by risk assessment results.
- Ensure policies are aligned with industry standards, legal requirements, and business objectives.

5. Implementation and Enforcement

- Assign dedicated resources for implementing cybersecurity programs and initiatives.
- Undertake security policy implementation and enforcement across all levels of the organization.
- Ensure regular training and awareness programs to support policy adherence.

6. Monitoring, Auditing, and Compliance

- Perform periodic risk assessments and update the risk mitigation strategy accordingly.
- Conduct regular reviews and updates of security policies to ensure they remain effective and relevant.
- Undertake internal audits for legal and regulatory compliance, focusing on adherence to cybersecurity laws and regulations.
- Perform regular audits for security policy compliance, ensuring policies are effectively implemented and followed.
- Implement continuous monitoring and improvement processes to adapt to emerging threats and vulnerabilities.

7. Stakeholder Engagement and Communication

- Identify and manage stakeholder collaboration, including partnerships with external entities and suppliers.
- Facilitate regular communication between cybersecurity teams and other business units to ensure alignment and transparency.

8. Incident Response and Recovery

- Develop and test incident response plans, ensuring they align with the broader governance framework.
- Include recovery strategies in the governance framework to ensure rapid restoration of operations post-incident.
- Establish metrics for incident response effectiveness and recovery time objectives (RTOs).

9. Continuous Improvement

- Incorporate continuous improvement mechanisms to refine cybersecurity governance practices over time.
- Regularly evaluate and adapt the governance framework based on feedback, new threats, and changes in business strategy.

10. Key Performance Indicators (KPIs)

- Define KPIs to measure the effectiveness of the cybersecurity governance framework across strategic, tactical, and operational levels.
- Regularly review and adjust KPIs to reflect the current threat landscape and organizational priorities.

6.2.4. Validation for the Proposed Framework

This section outlines the validation methodology for the proposed Cybersecurity Governance framework. The validation process aims to assess the effectiveness, efficiency, and suitability of the framework for its intended purpose. By rigorously evaluating the framework's performance, we can ensure its reliability and applicability in real-world scenarios. The validation methodology will involve a series of comprehensive tests and evaluations. Below is a description of how to validate the framework.

Table 6-4 Validation of the proposed framework

Validation Aspect	Objective	Validation Approach
Alignment with NIST CSF and Industry Standards	Confirm alignment with NIST CSF and relevant industry standards.	• **Mapping Exercise**: Map each framework category to NIST CSF functions (Identify, Protect, Detect, Respond, Recover). • **Gap Analysis**: Identify areas of misalignment with NIST CSF or ISO/IEC 27001 and address discrepancies.
Stakeholder Review and Feedback	Ensure the framework meets stakeholder needs (senior leadership, IT, legal, compliance).	• **Workshops and Interviews**: Gather feedback on framework aspects like Senior Leadership Commitment and Governance Structures. • **Surveys**: Distribute surveys within the organization for additional insights.
Pilot Implementation and Testing	Test the framework in a controlled environment to evaluate effectiveness.	• **Pilot Projects**: Implement the framework in a specific department to observe practical application. • **Tabletop Exercises**: Simulate cybersecurity incidents to test Incident Management Strategy and Response Planning.
Compliance and Regulatory Review	Ensure framework supports compliance with legal and regulatory requirements.	• **Legal and Regulatory Audit**: Verify framework components meet applicable laws and regulations. • **External Review**: Engage legal experts to assess the framework for regulatory risk mitigation.
Risk-Based Assessment	Validate the framework's effectiveness in	• **Risk Assessment**: Conduct a cybersecurity risk assessment focusing on categories like Risk Mitigation Strategies.

	managing cybersecurity risks.	• **Scenario Testing**: Use risk scenarios to test framework resilience against various threats.
Continuous Monitoring and Feedback Loop	Establish ongoing monitoring to keep the framework relevant.	• **Monitoring Mechanisms**: Implement tools to track performance using metrics like incident response times. • **Periodic Reviews**: Schedule regular reviews to incorporate lessons learned and updates.
External Validation and Benchmarking	Obtain an objective assessment of framework effectiveness from external experts.	• **Third-Party Audits**: Engage cybersecurity consultants to review framework areas like Business Continuity Planning. • **Benchmarking**: Compare the framework with similar frameworks in other organizations.
Documentation and Reporting	Ensure comprehensive documentation and effective communication of validation results.	• **Detailed Documentation**: Document the framework's design and validation process. • **Reporting to Leadership**: Prepare detailed reports summarizing validation findings for senior leadership and the board.

In addition to the given validation methodologies, case scenarios are presented below to demonstrate how the proposed cybersecurity governance framework operates in real-world situations involving cyber incidents. These scenarios provide practical examples of the framework's effectiveness in mitigating and responding to various security threats. By simulating potential security breaches and outlining how the framework would handle these incidents, the scenarios validate its applicability and robustness. This combination of theoretical validation and real-world case studies strengthens the overall credibility and effectiveness of the proposed framework.

6.2.5. ENIDP Scenario or Case-Based Framework Implementation

Scenario - 1

Scenario 1: Responding to a Ransomware Attack on the NID Program

Context:

A ransomware attack targets the National Identification program, encrypting critical databases containing citizen information and demanding payment for decryption. This incident threatens the availability and integrity of the NID system, with severe implications for the public and government operations.

1. **Govern Phase**

Goal: Ensure leadership and governance structures guide the response to the ransomware attack.

- **Senior Leadership Commitment:** Senior leaders prioritize the incident, mobilizing resources, and making critical decisions to manage the ransomware attack. They ensure all actions are aligned with the organization's goals and legal obligations.
- **Governance Structures:** The incident response team, along with crisis management structures, are activated to lead the effort in containing and mitigating the attack, with clear roles and responsibilities across the organization.
- **Cybersecurity Policy and Strategy Reviews:** Policies are reviewed to address weaknesses exposed by the ransomware attack, including enhancing data backup strategies, incident response protocols, and access controls.

Outcome: A coordinated, leadership-driven approach ensures swift decision-making and resource allocation to manage the ransomware attack effectively.

2. Identify Phase

Goal: Accurately assess the scope and impact of the ransomware attack.

- **Risk Assessment:** Conduct a detailed risk assessment to determine the extent of the attack, including identifying the systems and data that have been compromised, the type of ransomware used, and the potential impact on operations.
- **Policy Enforcement:** Enforce existing policies to isolate affected systems, prevent further spread, and protect unaffected systems.
- **Compliance Check:** Ensure that all legal and regulatory requirements are met, including notifying authorities, stakeholders, and potentially affected individuals about the ransomware attack.

Outcome: The scope of the ransomware attack is fully understood, and the risk is contained to prevent further damage.

3. Protect Phase

Goal: Implement immediate measures to prevent further spread and secure critical assets.

- **Risk Mitigation Strategies:** Isolate affected systems, disconnect them from the network, and initiate data backup and recovery procedures. Strengthen endpoint security across the organization to prevent further compromise.
- **Technology Integration:** Deploy security tools like endpoint detection and response (EDR) systems, anti-malware software, and network segmentation to limit the attack's spread and protect unaffected systems.
- **Stakeholder Engagement:** Engage key stakeholders, including IT teams, legal advisors, and communication teams, to ensure a unified response and clear communication about the situation.

Outcome: The ransomware is contained, and critical systems are protected from further compromise.

4. Detect Phase

Goal: Ensure rapid detection of the ransomware attack and ongoing monitoring for any additional threats.

- **Continuous Monitoring:** Use real-time monitoring tools to detect any signs of ransomware activity across the network, including attempts to spread or exfiltrate data.
- **Audit Insights:** Review system logs, threat intelligence, and audit data to identify the attack vectors used and assess any missed security gaps that contributed to the incident.

Outcome: The ransomware attack is detected early, and ongoing monitoring provides insights to guide the response.

5. Respond Phase

Goal: Execute a coordinated response to manage and mitigate the ransomware attack.

- **Incident Management Strategy:** Activate the incident response plan tailored for ransomware, focusing on containment, eradication, and recovery. Teams work together to clean affected systems, restore data, and return operations to normal.
- **Communication Plan:** Implement a clear communication strategy to inform employees, stakeholders, and the public about the attack, outlining the steps being taken and advising them on how to protect themselves from any related threats.
- **Reporting:** Document all actions taken during the response, including communication, containment, and recovery efforts. Ensure compliance with legal and regulatory requirements for incident reporting.

Outcome: The ransomware attack is effectively managed, and stakeholders are kept informed, reducing the impact on operations and public trust.

6. Recover Phase

Goal: Restore normal operations and build resilience against future ransomware attacks.

- **Business Continuity Planning:** Execute business continuity plans to maintain critical operations while restoring affected systems. Restore encrypted data from secure backups to minimize downtime and data loss.
- **Post-Incident Review:** Conduct a thorough review of the attack, including how it occurred, the effectiveness of the response, and any lessons learned. Use these insights to improve ransomware defenses, update incident response plans, and enhance backup strategies.
- **Awareness and Training:** Provide targeted training for employees on recognizing and preventing ransomware attacks, emphasizing the importance of security best practices and continuous vigilance.

Outcome: Normal operations are restored, data is recovered, and the organization's resilience against future ransomware attacks is significantly enhanced through improved processes and training.

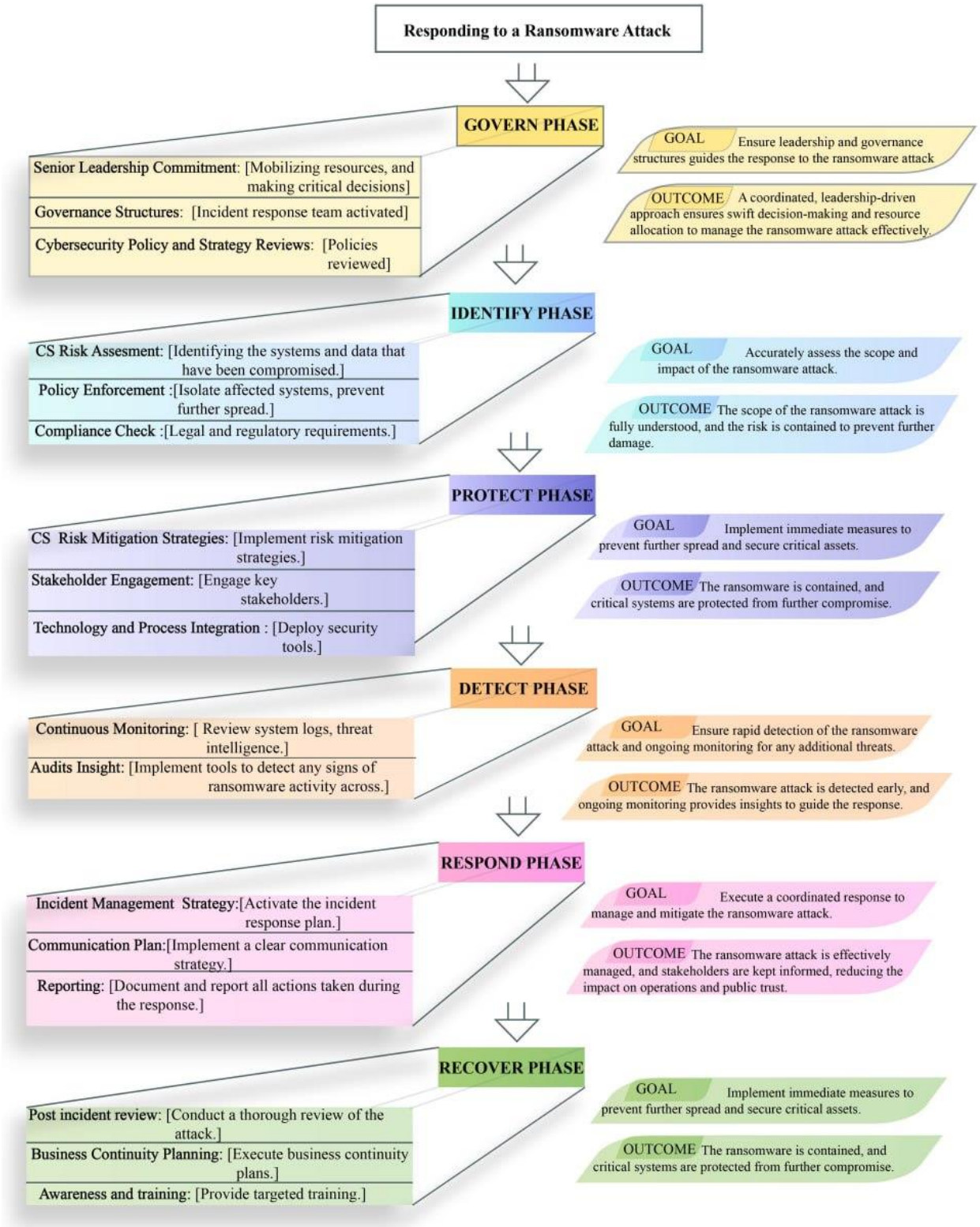

Figure 6-7 Responding to Ransomewahre Attack

Scenario 2

Scenario 2: Addressing Data Fraud or Errors in the NID Program

Context:

A significant issue is detected in the National Identification program involving fraudulent data entries and errors in citizen information. These issues are compromising the integrity of the NID system, leading to a loss of trust among citizens and potential legal implications. The cybersecurity framework is applied to address and resolve these data fraud or error incidents effectively.

1. Govern Phase

Goal: Establish robust governance and leadership to manage data fraud and errors effectively.

- **Senior Leadership Commitment:** Leadership is actively engaged in addressing data fraud and errors, ensuring that the response aligns with organizational priorities, and dedicating resources to mitigate the impact.
- **Governance Structures:** Activate governance frameworks to oversee the investigation and resolution of data fraud and errors. Assign clear roles and responsibilities for incident management across different teams.
- **Cybersecurity Policy and Strategy Reviews:** Review and update policies to tighten data entry procedures, enhance verification processes, and prevent unauthorized access. Policies should emphasize data integrity and accountability.

Outcome: A well-coordinated governance approach ensures that data fraud and errors are addressed systematically, with strong leadership and policy alignment.

2. Identify Phase

Goal: Accurately identify and assess the scope of data fraud or errors to facilitate corrective action.

- **Risk Assessment:** Conduct a thorough risk assessment to determine the extent of fraudulent data entries and errors, identify compromised records, and evaluate potential threats to the system's integrity.
- **Policy Enforcement:** Enforce policies to immediately halt any ongoing data fraud or errors. Implement stricter controls on data access and entry processes to prevent further incidents.
- **Compliance Check:** Ensure that all actions taken are in compliance with relevant legal and regulatory requirements, particularly regarding data accuracy, citizen rights, and privacy protections.

Outcome: Data fraud and errors are fully identified, and the necessary policies are enforced to contain and address the problem.

3. **Protect Phase**

Goal: Strengthen measures to protect the NID program from data fraud and errors.

- **Risk Mitigation Strategies:** Implement immediate risk mitigation strategies, such as enhanced data validation checks, secure data entry protocols, and restricted access to sensitive data.
- **Technology Integration:** Use advanced technology tools, such as automated data verification systems and encryption, to protect data from fraud and errors. Ensure all processes are integrated for a streamlined approach.
- **Stakeholder Engagement:** Engage key stakeholders, including government agencies, data management teams, and the public, to ensure they are informed and aligned in protecting data integrity.

Outcome: The NID program is fortified against data fraud and errors, with technology and stakeholders supporting protection efforts.

4. **Detect Phase**

Goal: Ensure timely detection of data fraud or errors and facilitate prompt corrective action.

- **Continuous Monitoring:** Deploy real-time monitoring tools to detect any irregularities or suspicious activities in the data management process. Quickly identify any new cases of fraud or errors.
- **Audit Insights:** Regularly audit data entry and management processes to identify vulnerabilities that could lead to errors or fraud. Use insights from audits to strengthen prevention measures.

Outcome: Data fraud and errors are detected early, allowing for swift and effective corrective actions.

5. Respond Phase

Goal: Manage and resolve incidents of data fraud or errors effectively.

- **Incident Management Strategy:** Deploy a pre-defined incident management strategy to address data fraud and errors. This includes steps for data correction, legal compliance, and communication with affected individuals.
- **Communication Plan:** Execute a communication plan that keeps stakeholders, including citizens, informed about the steps being taken to resolve the issue. Maintain transparency to rebuild trust.
- **Reporting:** Document all actions taken to resolve the data fraud or errors. Ensure thorough reporting for compliance, review, and continuous improvement.

Outcome: Data fraud and errors are resolved efficiently, with clear communication and comprehensive documentation ensuring accountability and transparency.

6. Recover Phase

Goal: Restore data integrity and strengthen resilience against future data fraud or errors.

- **Business Continuity Planning:** Ensure that the NID program can continue to function smoothly while addressing data fraud or errors. Implement contingency plans to minimize disruptions during the recovery phase.
- **Data Restoration:** Correct erroneous data and remove fraudulent entries, ensuring data integrity is fully restored. Use secure backups if necessary to recover accurate data.
- **Post-Incident Review:** Conduct a post-incident review to identify lessons learned from the incident. Use these insights to refine the cybersecurity framework and improve future data management processes.

Outcome: The integrity of the NID data is fully restored, and the program is better equipped to prevent and manage future incidents of data fraud or errors.

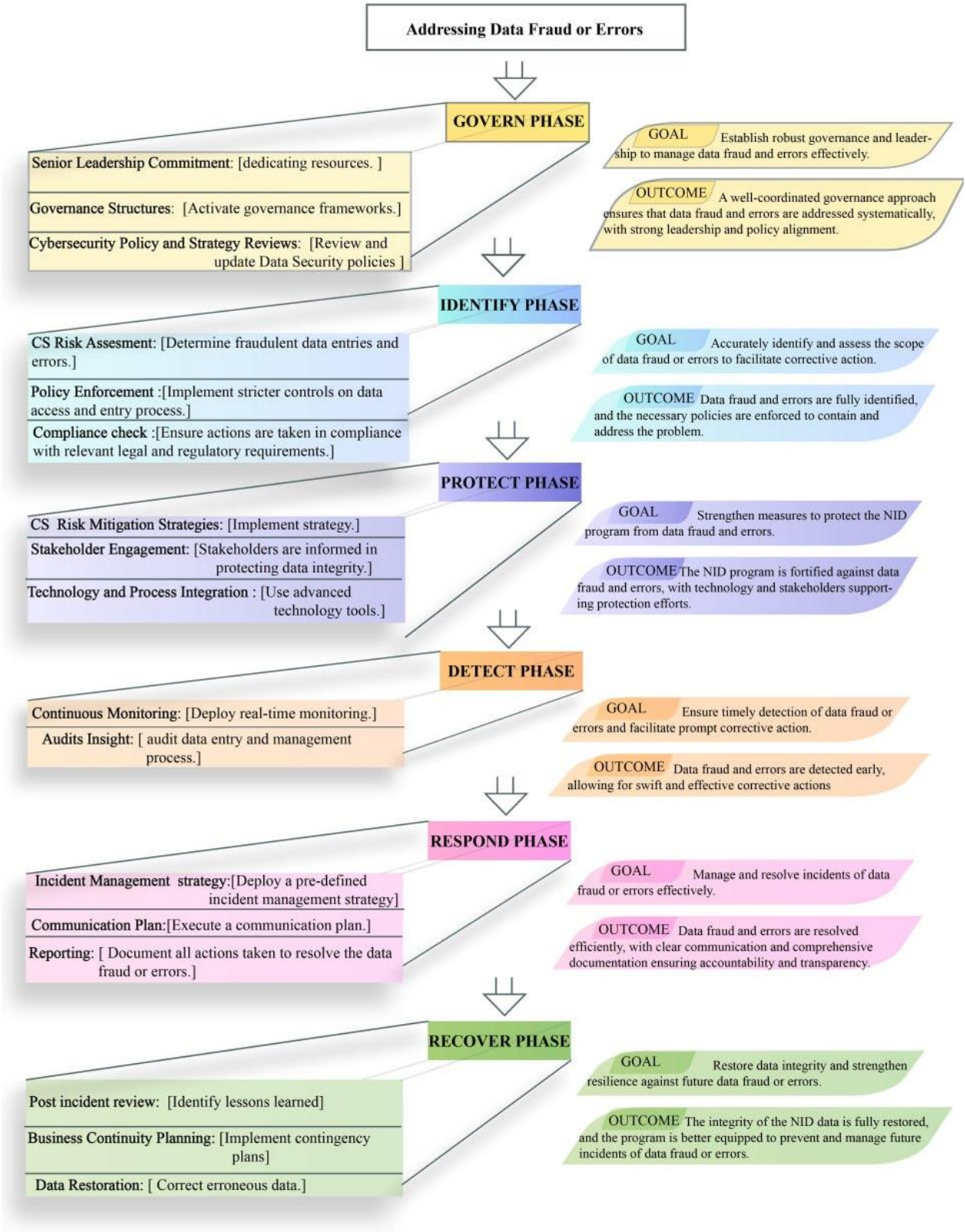

Figure 6-8 Addressing Data Fraud or Errors

Senario 3

Scenario 3: Responding to a DDoS Attack on NID Program

Context:

The National Identification program experiences a Distributed Denial of Service (DDoS) attack. Attackers flood the NID servers with a massive volume of traffic, overwhelming the system and causing significant disruption to public services that rely on the NID infrastructure.

1. **Govern Phase**

Goal: Ensure leadership is fully engaged and the incident response is well-coordinated.

- **Senior Leadership Commitment:** Top leadership prioritizes the incident, allocating the necessary resources and authority to the incident response team.
- **Governance Structures:** The established incident response team is activated, with clear roles and responsibilities for managing the DDoS attack.
- **Cybersecurity Policy and Strategy Reviews:** Policies related to network traffic management and response to service outages are reviewed and updated to enhance resilience.

Outcome: A coordinated and leadership-driven response framework that ensures effective management of the DDoS attack.

2. **Identify Phase**

Goal: Quickly identify the nature and scope of the DDoS attack.

- **Risk Assessment:** Analyze network traffic patterns to confirm the presence of a DDoS attack, determine the attack vectors, and assess its impact on NID services.
- **Policy Enforcement:** Enforce existing security protocols, such as traffic filtering and rate limiting, to mitigate the attack.
- **Compliance Check:** Verify that the organization meets legal and regulatory obligations, including notifying relevant authorities and stakeholders about the disruption.

Outcome: The DDoS attack is accurately identified, enabling the deployment of appropriate countermeasures.

3. **Protect Phase**

Goal: Implement measures to mitigate the impact of the DDoS attack.

- **Risk Mitigation Strategies:** Activate DDoS protection services, such as traffic scrubbing and load balancing, to manage the increased traffic and maintain service availability.
- **Technology Integration:** Utilize advanced DDoS protection tools, such as intrusion prevention systems (IPS) and web application firewalls (WAF), to filter malicious traffic.
- **Stakeholder Engagement:** Communicate with ISPs and other relevant stakeholders to collaborate on mitigating the attack and rerouting legitimate traffic.

Outcome: The impact of the DDoS attack is minimized, and essential services are protected from complete shutdown.

4. **Detect Phase**

Goal: Ensure continuous monitoring and detection of ongoing attack activity.

- **Continuous Monitoring:** Deploy real-time monitoring tools to track the attack's progress, measure traffic patterns, and identify any changes in attack tactics.
- **Audit Insights:** Review network and system logs to detect any anomalies or precursor activities that may have indicated the attack.

Outcome: Continuous monitoring provides real-time insights into the attack, enabling quick adjustments to defense strategies.

5. **Respond Phase**

Goal: Effectively manage the response to the DDoS attack and restore normal services.

- **Incident Management Strategy:** Execute a predefined DDoS response plan, focusing on traffic rerouting, server load distribution, and collaboration with third-party security services.
- **Communication Plan:** Inform key stakeholders, including government entities, service users, and the public, about the attack and ongoing mitigation efforts to maintain transparency and trust.
- **Reporting:** Document the attack, response actions, and communication for regulatory compliance and post-incident analysis.

Outcome: The attack is managed effectively, maintaining partial service availability and minimizing the impact on users.

6. **Recover Phase**

Goal: Restore full service functionality and strengthen defenses against future DDoS attacks.

- **Business Continuity Planning:** Execute recovery plans to gradually restore full-service availability, prioritizing critical functions and services first.
- **Technology and Process Integration:** Review and upgrade DDoS mitigation **technologies**, incorporating lessons learned to bolster future defenses.
- **Post-Incident Review:** Conduct a comprehensive analysis of the attack to identify areas for improvement in detection, response, and protection strategies.

Outcome: Full services are restored, and the organization's resilience to future DDoS attacks is enhanced through improved practices and technologies.

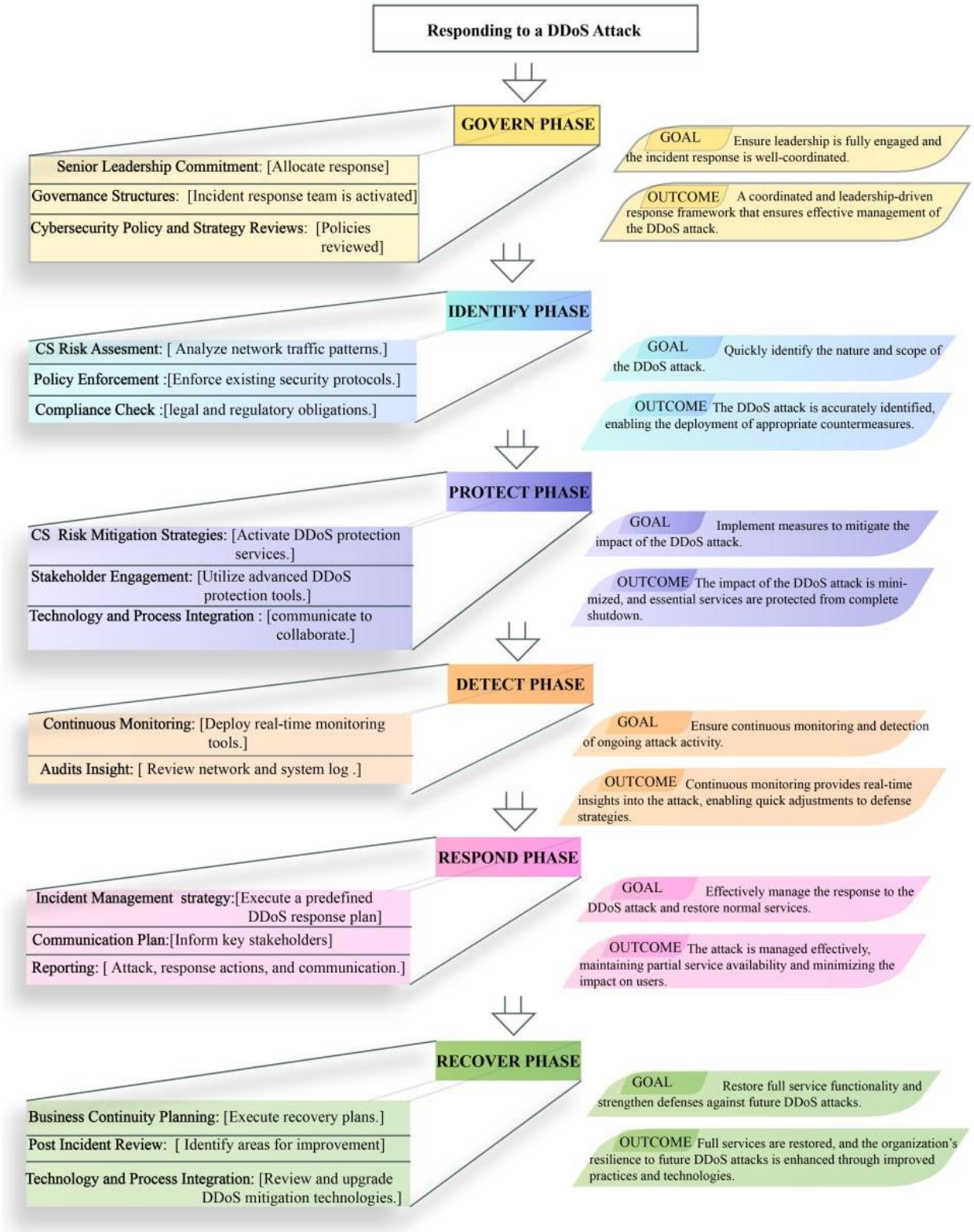

Figure 6-9 Responding to a DDoS Attack

Scenario 4

Scenario 4: Grievance and Complaint Redressal in the NID Program

Context:

A significant number of complaints arise from citizens regarding issues such as delayed processing, errors in identification documents, and data inaccuracies in the National Identification program. The situation is escalating, with public dissatisfaction potentially undermining the credibility of the NID system. The cybersecurity framework is used to address these grievances efficiently, ensure transparency, and restore trust.

1. Govern Phase

Goal: Establish a governance framework to manage grievances and complaints effectively.

- **Senior Leadership Commitment:** Leadership ensures that the grievance redressal process is a priority, with dedicated resources and a clear mandate to resolve issues promptly and transparently.
- **Governance Structures:** Activate governance structures that include a grievance redressal committee to oversee the process. Ensure that roles and responsibilities are clearly defined for handling complaints.
- **Cybersecurity Policy and Strategy Reviews:** Review policies related to data management, user rights, and service delivery to address the root causes of complaints. Ensure these policies align with the organization's mission of delivering a reliable and secure NID system.

Outcome: Leadership-driven and well-structured governance ensures that grievance redressal is approached systematically, with a focus on transparency and accountability.

2. Identify Phase

Goal: Accurately assess the nature and scope of grievances to ensure timely resolution.

- **Risk Assessment:** Conduct an assessment to categorize the grievances, identify patterns, and determine the severity of the issues. Evaluate whether the complaints are linked to systemic flaws, cybersecurity breaches, or operational inefficiencies.
- **Policy Enforcement:** Enforce policies to promptly address data inaccuracies, delayed processing, and other issues raised by citizens. Ensure that corrective measures are implemented.
- **Compliance Check:** Ensure that the grievance redressal process complies with legal and regulatory requirements, including data protection laws and customer service standards.

Outcome: Grievances are thoroughly understood, categorized, and addressed within the framework of existing policies and legal requirements.

3. Protect Phase

Goal: Implement measures to prevent future grievances and protect citizen data.

- **Risk Mitigation Strategies:** Strengthen data management practices, improve verification processes, and enhance system reliability to minimize errors and delays that lead to grievances.
- **Technology Integration:** Use technology to automate parts of the grievance redressal process, such as online complaint submission and tracking, to ensure timely responses and transparency.
- **Stakeholder Engagement:** Engage key stakeholders, including government agencies, civil society, and the public, to gather feedback and improve the NID system's responsiveness to citizen needs.

Outcome: Measures are in place to prevent recurring issues, protect citizen data, and maintain public confidence in the NID program.

4. Detect Phase

Goal: Identify and monitor emerging grievances and complaints proactively.

- **Continuous Monitoring:** Monitor complaints in real-time using analytics tools that detect trends and emerging issues, enabling quick responses to prevent escalation.
- **Audit Insights:** Regularly review and audit the grievance redressal process to ensure it is effective, identify any missed issues, and adjust the process as necessary.

Outcome: Emerging grievances are detected early, and the organization can respond quickly to resolve issues before they become widespread.

5. **Respond Phase**

Goal: Address grievances and complaints promptly and transparently.

- **Incident Management Strategy:** Activate the incident management strategy for handling grievances, ensuring that responses are coordinated across departments, and issues are resolved promptly.
- **Communication Plan:** Develop a communication plan to keep complainants informed about the status of their grievances, explaining the steps being taken to resolve them and setting realistic expectations.
- **Reporting:** Document all grievance redressal activities, ensuring that actions taken are recorded for future reference, compliance, and continuous improvement.

Outcome: Grievances are resolved effectively, with clear communication and documentation that enhances public trust and satisfaction.

6. **Recover Phase**

Goal: Restore public trust and continuously improve the grievance redressal process.

- **Business Continuity Planning:** Ensure that the grievance redressal process continues to function even during disruptions, such as system downtime or staff shortages, by having contingency plans in place.

- **Post-Incident Review:** After resolving grievances, conduct a review to identify lessons learned, systemic issues, and opportunities for improvement in the grievance redressal process.
- **Awareness and Training:** Educate staff and the public about the grievance redressal process, emphasizing the importance of timely reporting and the role of citizens in helping to improve the NID system.

Outcome: Trust in the NID program is restored, the grievance redressal process is refined and the system is better prepared to handel future complaints.

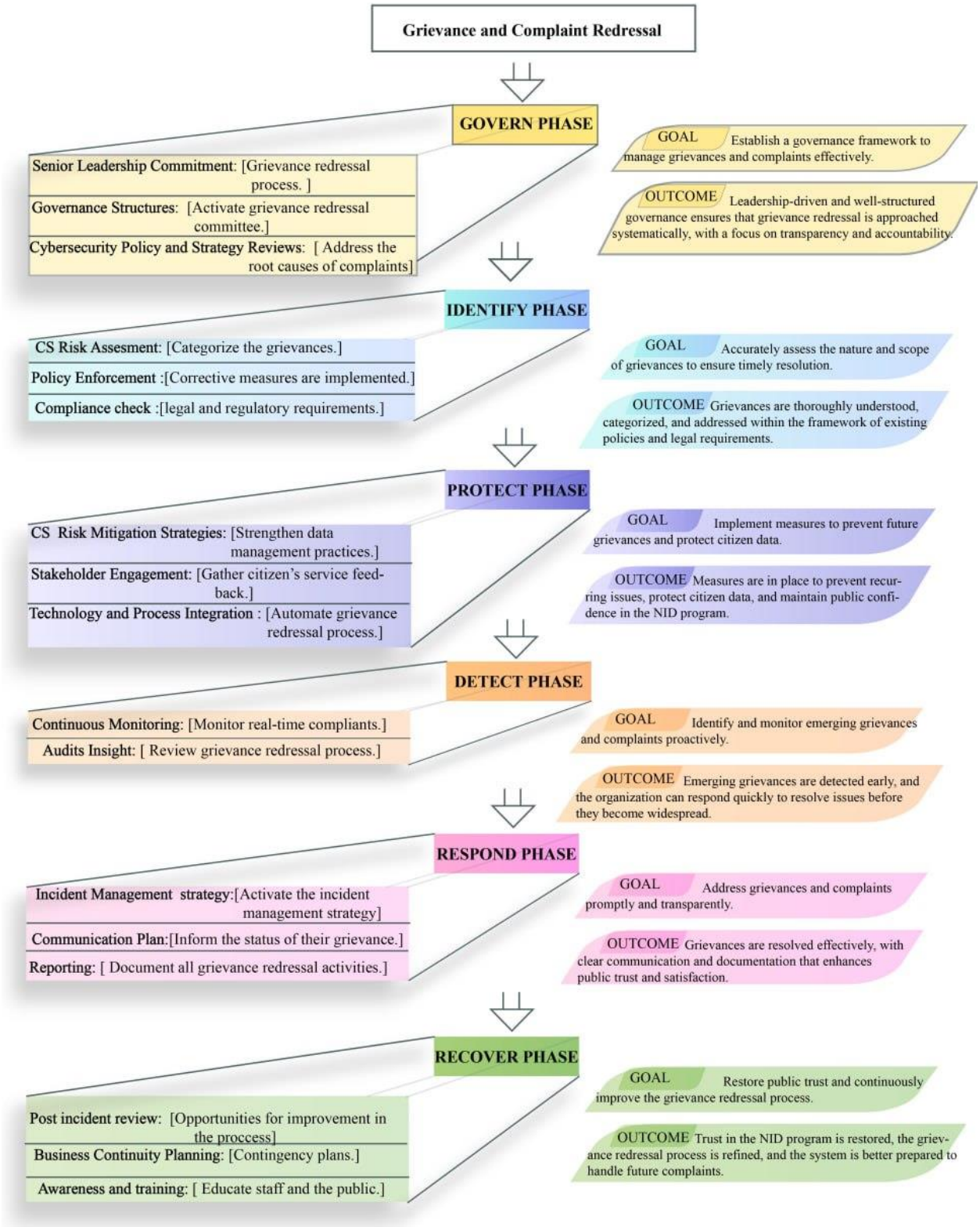

Figure 6-10 Griviance and Compliant Redressal

6.3. Limitations

One limitation of this research is the insufficient existing literature on cybersecurity governance specifically related to national digital identification programs. Furthermore, this framework has not yet been tested in real-world environments but only ways of how to validate and incident scenarios are provided. However, utilizing the internationally recognized NIST standard as a foundation and integrating it with leadership hierarchies is anticipated to enhance overall security. While developing a new framework from scratch has its merits, leveraging an established, well-tested framework allows for building on existing standards and minimizes the need for extensive testing.

6.4. Future Work

The future work will focus on piloting the proposed cybersecurity governance framework across various sectors beyond the national identification program, including critical infrastructure environments, to assess how effectively it addresses key cybersecurity governance aspects. Additionally, the framework will be tested in organizations of different sizes, such as small-to-medium enterprises (SMEs) and larger corporations, to explore how it can be tailored to meet the specific needs and challenges of diverse organizational structures.

References

1. Abbadia, J. (2022, October 3). *esearch Paradigm: An Introduction with Examples*. Retrieved from https://mindthegraph.com:https://mindthegraph.com/blog/research-paradigm/#:~:text=What%20is%20a%20research%20paradigm,research%20methodologies%3A%20positivism%20or%20interpretivism.

2. Akuetteh, S. O.-M. (2021). *Digital Identity in Ghana.* Cape Town: Centre for Internet and Society (CIS) and Research ICT Africa (RIA).

3. Alan Bryman, &. E. (2015). *Business Research Methods.* Oxford : Oxford University Press.

4. Alina, M. A. (2016). Securing the Internet of Things: a Review. *Issues In Information Systems, 17*(Iv), 21-28. doi:10.48009/4_iis_2016_21-28

5. Alkhurayyif, Y. (May 2013). Security Concerns with National ID Cards. *ResarchGate*, 44-48.

6. *All-in-One Qualitative Data Analysis Software*. (2023, 02 15). Retrieved from https://www.maxqda.com:https://www.maxqda.com/qualitative-data-analysis-software?gclid=EAIaIQobChMIwdP06byX_QIVhRh9Ch0vTQgrEAAYASAAEgIkBfD_BwE

7. Al-Mashhadi, A. D. (2023). Methodologies, Requirements and Challenges of Cybersecurity Frameworks: A Review. *International Journal of Wireless and Microwave Technologies, 13*(1), 1-13. doi:10.5815/ijwmt.2023.01.01

8. Alqatawna, J. (2014). The Challenge of Implementing Information Security Standards in Small and Medium e-Business Enterprises. *Scientific Reesarch Open Access*. Retrieved from https://www.scirp.org: https://www.scirp.org/html/7-9301952_49991.htm

9. Andy, L. B. (2012). Selecting a Research Topic : A Framework for Doctoral Students.

10. Babatunde, O. (2021). *Digital Identity in Nigeria.* Cape Town: Centre for Internet and Society (CIS) and Research ICT Africa (RIA).

11. Babikian, J. (February 2024). Securing Rights: Legal Frameworks for Privacy and Data Protection in the Digital Era. *Law Research Journal P-ISSN: 3006-3027, E-ISSN: 3006-3035*, 91-98.

12. Badi, S. A. (2020). The Role of Governance in Achieving Sustainable Cybersecurity for Business Corporations. *Journal of Information Security and Cybercrimes Research, 3*(1), 97-112. doi:10.26735/eint7997

13. Badi, S. A. (2020). The Role of Governance in Achieving Sustainable Cybersecurity for Business Corporations Business Corporations. *JISCR*, 98-110.

14. Benjamin, S. J. (2017). Saturation in qualitative research: exploring its conceptualization and operationalization. *National Library of Medicine*, 1893-1907.

15. Bhandari, P. (2023). *What Is Qualitative Research? | Methods & Examples. Scribbr.* Retrieved from https://www.scribbr.com/methodology/qualitative-research/

16. Bhandari, V. a. (2020, March 01). Governing ID: Principles of Evaluation. *Centre for Internet & Society*, 30. Retrieved from https://ssrn.com/abstract=3774917

17. Bigelow, S. J. (2024, 04 12). *ITIL (Information Technology Infrastructure Library)*. Retrieved from https://www.techtarget.com: https://www.techtarget.com/searchdatacenter/definition/ITIL#:~:text=ITIL%20(Information%20Technology%20Infrastructure%20Library)%20is%20a%20framework%20designed%20to,and%20achieve%20predictable%20service%20delivery.

18. Biji Scaria. (2022, February 3). *The Importance of a National Digital Identity System*. Retrieved from https://www.isaca.org: https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/the-importance-of-a-national-digital-identity-system

19. Bin Srinidhi, J. Y. (2015). Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. *ELSEVIER*, 49-62.

20. Binda, D. E. (2023). *Digital Identity in Rwanda.* Cape Town: Research ICT Africa and Centre for Internet and Society.

21. Boshe, P. (2023). *Digital Identity in Tanzania.* Cape Town: Research ICT Africa and Centre for Internet and Society.

22. Boutwell, M. B. (2019). Exploring Industry Cybersecurity Strategy in Protecting Critical Infrastructure.

23. Bowen, G. A. (2009). Document Analysis as a Qualitative Research Method. *ualitative Research Journal, vol. 9, no. 2, pp. 27-40. DOI 10.3316/QRJ0902027. ,* 28-38.

24. Braun, V. C. (2016). Thematic analysis. *The Journal of Positive Psychology* , 297-298 .

25. Breckenridge, K. (2014, October). Biometric State: The Global Politics of Identification and Surveillance in South Africa, 1850 to the present. *72*. doi:https://doi.org/10.1017/CBO9781139939546

26. Broadman, H. G. (2018, 11 28). *Corporate Boards' Oversight Of Cyber Risks Is Too Passive.* Retrieved from Https://Www.Forbes.Com/Sites/Harrybroadman/2018/11/28/Corporate-Boards-Oversight-of-Cyber-Risks-Is-Too-Passive/#45ad65ef1f81

27. Bryman, E. B. (2007). The Ethics of Management Research: An Exploratory Content Analysis. *ResearchGate*, 63 - 77.

28. Camp, W. G. (2001). Formulating and Evaluating Theoretical Frameworks for Career and Technical Education Research. *26*(1), 4-25.

29. centraleyes. (2023, 01 17). *Cyber Governance*. Retrieved from https://www.centraleyes.com: https://www.centraleyes.com/glossary/cyber-governance/

30. Chan, H. T. (2015, November 24). *Benefits, concerns around national identification systems*. Retrieved from https://www.hsph.harvard.edu: https://www.hsph.harvard.edu/news/features/benefits-concerns-around-national-identification-systems/

31. Cherilyn Pascoe, S. Q. (2024, February 26). The NIST Cybersecurity Framework (CSF) 2.0. *NIST*. doi:10.6028/NIST.CSWP.29

32. CISA. (2024, 04 13). *Cybersecurity Governance*. Retrieved from https://www.cisa.gov: https://www.cisa.gov/topics/cybersecurity-best-practices/cybersecurity-governance#:~:text=Cybersecurity%20governance%20is%20a%20comprehensive,to%20cyber%20threats%20or%20attacks.

33. CISCO. (2024, 05 3). *What Is the NIST Cybersecurity Framework?* Retrieved from https://www.cisco.com: https://www.cisco.com/c/en/us/products/security/what-is-nist-csf.html

34. Cisternelli, E. (2024, February 27). *7 Cybersecurity Frameworks That Help Reduce Cyber Risk (List & Resources)*. Retrieved from https://www.bitsight.com: https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk

35. citizenshiprightsafrica. (2023, April 3). *Ethiopian National ID Program*. Retrieved from http://citizenshiprightsafrica.org: http://citizenshiprightsafrica.org/wp-content/uploads/Ethiopian-National-ID-Program-Apr2023.pdf

36. Clark, B. V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3(2), https://doi.org/10.1191/1478088706qp063oa*, 77–101.

37. Cofta, P. (2008). *Identity in the Information Society, Volume 1*(1), 39-53. doi:10.1007/s12394-009-0006-6

38. ComplianceForge. (2022). *Integrated Controls Management (ICM) – Plan, Do, Check & Act (PCDA) Approach.* Retrieved from https://graphics.complianceforge.com: https://graphics.complianceforge.com/icm/ICM-PCDA.pdf

39. Crane, W. (2012). *Principles and Methods of Social Research. 2nd ed.* Boston: Allyn and Bacon.

40. Creswell, J. (2013). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. 4th Edition.* London: SAGE Publications, Inc.

41. David, L. M. (1998). *Planning Focus Groups.* Sage Publications Inc.

42. Deb Bodeau, S. B.-G. (September 2010). *Cyber Security Governance: A Component of MITRE's Cyber Prep.* MITRE.

43. Diogo Proen, R. V. (2016). 15-26. doi:10.1007/978-3-319-43997-6

44. Diyal, R. P. (November 2023). A Study on the Situation of National Identity Card in Nepal: implications and challenges. *EDUCATIONAL JOURNAL VOL.: 2 ISSUE: 2*, 10-23.

45. Dr. Elvis M. Binda. (2021). *Digital Identity in Rwanda.* Cape Town: Research ICT Africa and Centre for Internet and Society.

46. EDIP. (2023). *Ethiopian Digital Identification Proclamation No. 1284/2023.* Addis Ababa: Federal Negarit Gazette.

47. *e-Identity*. (2024, 04 18). Retrieved from https://e-estonia.com: https://e-estonia.com/solutions/estonian-e-identity/e-residency/

48. Emma, B. A. (2018). *Business Research Methods.* Oxford: Oxford University Press.

49. ENIDP. (2023, 01 18). *Digital ID Services*. Retrieved from https://id.gov.e: https://id.gov.et/en/services/

50. ENIDP. (2023, 01 21). *National ID History*. Retrieved from https://id.gov.et: https://id.gov.et/en/history/

51. ENISA. (2017). *Cyber Security Culture in organisations* (Vol. 46). Anasthesiologie und Intensivmedizin. doi:10.2824/10543

52. Erikson, E. H. (1994). *Identity and the life cycle.* New York: WW Norton & company.Inc.

53. Ethiopian Business Review. (2024, January 15). *Empowering Citizens Unveiling Ethiopia's National ID Programme*. Retrieved from https://ethiopianbusinessreview.net: https://ethiopianbusinessreview.net/empowering-citizens-unveiling-ethiopias-national-id-programme/

54. Eugen, P. (2018). Exploring the New Era of Cybersecurity Governance. *Ovidius University Annals, Economic Sciences Series, XVIII*(1), 358-363.

55. European Commission. (2024, 04 15). *DIGITAL eID* . Retrieved from https://ec.europa.eu: https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/eID

56. Fagerström, A. (2013). Creating , Maintaining and Managing an Information Security Culture.

57. Falconer, S. O.-M. (2023). *Digital Identity in Ghana.* Cape Town: Centre for Internet and Society (CIS) and Research ICT Africa (RIA).

58. FG DFS. (2016). *Review of National Identity Programs.* ITU-T.

59. Fonceca, C. M. (April 2023). Cyber security culture in an IT company: An empirical study. *International Journal of Multidisciplinary Research and Growth Evaluation ISSN (online): 2582-7138, Volume: 04,Issue: 02*, 351-354.

60. Gabriella, R. (2021). *Digital Identity in South Africa.* Cape Town: Centre for Internet and Society (CIS) and Research ICT Africa (RIA).

61. Gavendra Singh, A. C. (2017). National Identification System in the Countries Around the Globe: an Outside Review From Ethiopian Perspective. *International Journal of Advanced Research*, 958-965.

62. Ghadge, M. N. (2024). Digital Identity in the Age of Cybersecurity:Challenges and Solutions. *London Journal of Research in Computer Science and Technology, Volume 24 | Issue 1 | Compilation 1.0, Print ISSN: 2514-863X, Online ISSN: 2514-8648*, 1-7.

63. Grace Mutung'u. (2021). *Digital Identity in Kenya.* Cape Town: Centre for Internet and Society (CIS) and Research ICT Africa (RIA).

64. Grant, C. (2015, April). Understanding, selecting, and integrating a theoretical framework in dissertation research: Developing a 'blueprint' for your "house". doi:10.5929/2014.4.2.9

65. Greg, G. K. (2012). *Applied Thematic Analysis.* SAGE.

66. Hafeez-Baig, S. Y. (2021). A Conceptual Model for Cybersecurity Governance. *Journal of Applied Security Research, 16*(4), 490-513. doi:10.1080/19361610.2021.1918995

67. Haile, D. (2023, October). *Ethiopia - Data Protection Overview*. Retrieved from https://www.dataguidance.com: https://www.dataguidance.com/notes/ethiopia-data-protection-overview

68. Harisaiprasad, K. (2020, April 27). *COBIT 2019 and COBIT 5 Comparison*. Retrieved from https://www.isaca.org: https://www.isaca.org/resources/news-and-trends/industry-news/2020/cobit-2019-and-cobit-5-comparison

69. Harvard T.H. Chan. (2015, November 24). *Benefits, concerns around national identification systems*. Retrieved from https://www.hsph.harvard.edu: https://www.hsph.harvard.edu/news/features/benefits-concerns-around-national-identification-systems/

70. Hedges, S. S. (2019, July 25). *https://insights.sei.cmu.edu/blog/cybersecurity-governance-part-1-5-fundamental-challenges/*. Retrieved from https://insights.sei.cmu.edu.

71. Hendrickson, L. (2024, June 10). *Why Are Governments Developing Digital ID Systems?* Retrieved from https://www.identity.com: https://www.identity.com/why-are-governments-developing-digital-id-systems/

72. IBM. (2023, 02 15). *IBM SPSS software*. Retrieved from https://www.ibm.com: https://www.ibm.com/spss?utm_content=SRCWW&p1=Search&p4=43700068092265910&p5=p&gclid=EAIaIQobChMI-pXW4buX_QIVJBV9Ch0onwadEAAYASAAEgJ9m_D_BwE&gclsrc=aw.ds

73. Ibrahim, M. (January 2015). The art of Data Analysis. *ResearchGate*, 99-104.

74. ICA. (2024, 02 14). *Register Identity Card for 15-year-olds*. Retrieved from https://www.ica.gov.sg: https://www.ica.gov.sg/documents/identity-cards

75. ID4D. (2022, 06 10). *Building Inclusive and Trusted ID systems to Empower People and Meet the SDGs*. Retrieved from https://id4d.worldbank.org: https://id4d.worldbank.org/node/2096

76. IEC. (2022, 08 15). *A governance framework for cyber security*. Retrieved from https://www.iec.ch: https://www.iec.ch/blog/governance-framework-cyber-security

77. intract. (2017). *Sampling.* intrac for civil society.

78. ISECUREDATA. (2023, Jan 26). *onquering the 5 Top Challenges of ISO 27001 Implementation in Small Businesses*. Retrieved from https://isecuredata.com: https://isecuredata.com/iso-27001-implementation-challenges-in-small-businesses/

79. ISO. (2024, 04 25). *ISO/IEC 27032:2023(en) Cybersecurity — Guidelines for Internet security*. Retrieved from https://www.iso.org: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-2:v1:en

80. IT Governance Ltd . (2024, 04 15). *What is COBIT 5? Definition & Explanation*. Retrieved from https://www.itgovernance.co.u: https://www.itgovernance.co.uk/cobit

81. IT Governance Ltd. (2024, 05 17). *Becoming Cyber Secure*. Retrieved from https://www.itgovernance.co.uk: https://www.itgovernance.co.uk/cybersecurity#:~:text=A%20cohesive%20approach%20to%20cyber,be%20managed%20by%20a%20process.

82. ITU-T X.1205. (2024, 03 13). *Definition of cybersecurity*. Retrieved from https://www.itu.int: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

83. Iyer, N. (2023). *Digital Identity in Uganda.* Cape Town: Research ICT Africa and Centre for Internet and Society.

84. Jabu Mtsweni, E. B. (2016). iSemServ: A model-driven approach for developing semantic web services. 55-69.

85. JACOB, B. J. (2018, February 27). *Pros and cons of national ID system*. Retrieved from https://www.gmanetwork.com: https://www.gmanetwork.com/news/opinion/content/644837/pros-and-cons-of-national-id-system/story/

86. Jan Vanhaecht, D. M. (2020, DEc 09). *https://www.deloitte.com/global/en/services/risk-advisory/perspectives/the-future-of-digital-identity.html*. Retrieved from https://www.deloitte.com: https://www.deloitte.com/global/en/services/risk-advisory/perspectives/the-future-of-digital-identity.html

87. Jan, v. B. (2020). Introduction to Design Science Research. 1-17.

88. Jansen, D. (2020, 05). *Qualitative Data Analysis Methods 101: The Big 6 Methods (Including Examples). Grad Coach.* Retrieved 05 16, 2023, from https://gradcoach.com/qualitative-data-analysis-methods/

89. Jerzak, C. T. (2015, November 12). *A Brief History of National ID Cards*. Retrieved from https://fxb.harvard.edu: https://fxb.harvard.edu/2015/11/12/a-brief-history-of-national-id-cards/

90. Jide Edu, M. H. (2023). Exploring the Risks and Challenges of National Electronic Identity (NeID) System. 1-5.

91. JONES, J. (2022, FEBRUARY 5). *COBIT 5 and Its Five Key Principles*. Retrieved from https://unichrone.com: https://unichrone.com/blog/it-governance/cobit-5-principles/

92. Joseph P. Simmons, L. D. (2011). False-Positive Psychology: Undisclosed Flexibility in Data Collection and Analysis Allows Presenting Anything as Significant. *Sage*.

93. Kabata, V. (February 2024). An assessment of the legal and regulatory framework supporting the implementation of the National Integrated Identity Management System (NIIMS) in Kenya.

94. Kaminsky, S. (2023, April 13). *Open source: the top-10 risks for business*. Retrieved from https://www.kaspersky.com: https://www.kaspersky.com/blog/open-source-top-10-risks/47875/

95. Karataş, S. S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. *International Cybersecurity Law Review, 3*(1), 7-34. doi:10.1365/s43439-021-00045-4

96. Kim, N. (2023). NATIONAL ID FOR PUBLIC PURPOSE. 273-297.

97. Kvale, S., & Flick, U. (2009). Doing interviews.

98. KvaleSteinar. (2007). Doing interviews. *Sage*.

99. Leigh, C. A. (2017). National ID Programs: A Multi-Country Review and Analysis of Policy and Practical Challenges. *AAAI Proceedings*, 1-5.

100. Lincoln, Y. S. (1985). Naturalistic inquiry. . *Sage Publications*.

101. Lorelli, S. N. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. *Sage*.

102. LPM. (November 2023). *Labor Management Procedures.* Addis Ababa: NIDP.

103. Luo, A. (2022, 12 05). *Content Analysis | Guide, Methods & Examples. Scribbr.* Retrieved 06 15, 2023, from https://www.scribbr.com/methodology/content-analysis/

104. Maayan, G. D. (2019, August 19). *https://securitytoday.com/Articles/2019/08/19/The-Dangers-of-OpenSource-Vulnerabilities-and-What-You-Can-Do-About-It.aspx?Page=1*. Retrieved from https://securitytoday.com: https://securitytoday.com/Articles/2019/08/19/The-Dangers-of-OpenSource-Vulnerabilities-and-What-You-Can-Do-About-It.aspx?Page=1

105. Mandy, M. A. (2019). Using Zoom Videoconferencing for Qualitative Data Collection: Perceptions and Experiences of Researchers and Participants. *Sage*.

106. Mani, V. (2019). Redefining Corporate Governance for Better Cyberrisk Management. *4*, 1-8.

107. Martins, P. G. (2021). *Digital Identity in Mozambique.* Cape Town: Centre for Internet and Society (CIS) and Research ICT Africa (RIA).

108. Martins, P. G. (2023). *Digital Identity in Mozambique.* Cape Town: Centre for Internet and Society (CIS) and Research ICT Africa (RIA).

109. Matthew N.O. Sadiku, A. E. (2016). Digital Identity. *TIJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3*, 86-97. doi:10.4324/9781003317524-9

110. McCombes, S. (2019 , September 19). *Sampling Methods | Types, Techniques & Examples*. Retrieved from www.scribbr.com: https://www.scribbr.com/methodology/sampling-methods/

111. Melaku, H. M. (2023). A Dynamic and Adaptive Cybersecurity Governance Framework. *MDPI*, 327–350.

112. Melody Musoni, E. D. (December 2023). *Digital ID systems in Africa:Challenges, risks and opportunities.* ecdpm.

113. Meyer, C. B. (2001). A Case in Case Study Methodology. *Sage*.

114. Michael, M. M. (1994). *Qualitative Data Analysis: An Expanded Source Book (2nd ed.).* Newbury Park, CA: Sage Publications, Inc.

115. Micro, T. (2012, January). The Human Factor in Data Protection Sponsored by Trend Micro.

116. Miles, M. B., & Huberman, A. M. (1994). *Qualitative Data Analysis: An Expanded Source Book (2nd ed.).* Newbury Park, CA: Sage Publications, Inc.

117. MIT. (2016, SEptember 07). *https://ide.mit.edu/insights/digital-identity-the-key-to-privacy-and-security-in-the-digital-world/*. Retrieved from https://ide.mit.edu.

118. MIT DIGITAL. (2016, September 07). *Digital Identity: The Key to Privacy and Security in the Digital World*. Retrieved from https://ide.mit.edu: https://ide.mit.edu/insights/digital-identity-the-key-to-privacy-and-security-in-the-digital-world/

119. Mojtaba, V. H. (2013). Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *National LIbrary of Medicine*, 398-405.

120. Morse, J. M. (1991). Approaches to Qualitative & Quantitative Methodological Triangulation. Nursing Research. *Journals A-Z, 40, https://doi.org/10.1097/00006199-199103000-00014*, 120-123.

121. MOSIP. (2023, 01 18). *An open source platform on which national foundational IDs are built*. Retrieved from https://mosip.io/: https://mosip.io/

122. MOSIP. (2023, 01 18). *An open source platform on which national foundational IDs are built*. Retrieved from https://mosip.io/: https://mosip.io/

123. Mutung'u, G. (2023). *Digital Identity in Kenya.* Cape Town: Centre for Internet and Society (CIS) and Research ICT Africa (RIA).

124. Neema Iyer. (2021). *Digital Identity in Uganda.* Cape Town: Research ICT Africa and Centre for Internet and Society.

125. Ngwenya, N. (2023). *Digital Identity in Zimbabwe.* Cape Town: Research ICT Africa and Centre for Internet and Society.

126. Nhlanhla Ngwenya. (2021). *Digital Identity in Zimbabwe.* Cape Town: Research ICT Africa and Centre for Internet and Society.

127. NID. (2022, Jan 17). *National ID Program of Ethiopia Announces a Pilot*. Retrieved from https://id.gov.et: https://id.gov.et/en/press-release-jan-2022/#:~:text=%E2%80%9CA%20national%20ID%20provides%20a,telecommunications%20services%20and%20more%2C%E2%80%9D%20said

128. NID. (2023, 01 18). *Digital ID Services*. Retrieved from https://id.gov.et: https://id.gov.et/en/services/

129. NID. (2023, 01 18). *NATIONAL ID STRATEGY*. Retrieved from https://id.gov.et: https://id.gov.et/en/strategy/

130. NID. (2023, 01 18). *NID Documetns*. Retrieved from https://id.gov.et: https://id.gov.et/en/documents/

131. NID. (2023, 01 21). *REGISTRATION FOR ENROLLMENT*. Retrieved from https://id.gov.et: https://id.gov.et/en/enrollment/

132. NISP. (September 2011). *The National Information Security POlicy.* Addis Ababa: Federal Democratic Republic of Ethiopia.

133. NIST. (February 2024). *The NIST Cybersecurity Framework (CSF) 2.0.* National Institute of Standards and Technology.

134. Nthabiseng Pule. (2021). *Digital Identity in Lestho.* Cape Town: Centre for Internet and Society (CIS) and Research ICT Africa (RIA).

135. Okunoye, B. (2020). *Digital Identity in Nigeria.* Cape Town: Centre for Internet and Society (CIS) and Research ICT Africa (RIA).

136. Olivia White, A. M. (2019, April). Digital Identification: A key to Inclusive Growth. *Mckinsey Global Institute*, 128. Retrieved from papers3://publication/uuid/A9CF25F1-866D-4036-AADB-7DE290E87A3F%5Cnpapers3://publication/uuid/42E08CE4-FA6E-4C93-A5FC-27381A3B56B2

137. Patricia Boshe. (2021). *Digital Identity in Tanzania.* Cape Town: Research ICT Africa and Centre for Internet and Society.

138. Patton, M. Q. (2002). *Qualitative Research & Evaluation Methods.* Sage.

139. PDPP. (2021). *Draft Personal Data Protection Prclamation.* Addis Ababa: Negarit Gazetta.

140. Pule, N. (2023). *Digital Identity in Lestho* . Cape Town: Centre for Internet and Society (CIS) and Research ICT Africa (RIA).

141. Pullin, D. W. (2018). Cybersecurity: Positive Changes Through Processes and Team Culture. *Frontiers of Health Services Management, 32*(1), 3-12. doi:10.1097/HAP.0000000000000038

142. QRP. (2021, 06 16). *The 7 ITIL 4 guiding principles*. Retrieved from https://www.qrpinternational.b: https://www.qrpinternational.be/blog/it-governance-and-service-management/the-7-itil-guiding-principles/

143. Razzano, G. (2023). *Digital Idneity in South Africa.* Cape Town: Centre for Internet and Society (CIS) and Research ICT Africa (RIA).

144. Renata M. de Carvalho, C. D. (2020). Protecting citizens' personal data and privacy: a joint effort from GDPR EU cluster research projects. *SN Computer Science 1(4), DOI: https://doi.org/10.1007/s42979-020-00218-8, Volume 1*(5), 1-2. doi:10.1007/s42979-020-00261-5

145. RSA. (2016). Cyber Risk Appetite: Defining and Understanding Risk in the Modern Enterprise. *RSA*, 1-4.

146. Ryerse, J. (2023, 02 03). *Top 11 cybersecurity frameworks in 2023*. Retrieved from https://www.connectwise.com: https://www.connectwise.com/blog/cybersecurity/11-best-cybersecurity-frameworks

147. S Roopa, M. R. (2017). Questionnaire Designing for a Survey. *JIOS*, 273-276.

148. SAIIA. (2025, 01 25). *Digital Identification and Biometrics In East Africa: Opportunities and Concerns*. Retrieved from https://saiia.org.za: https://saiia.org.za/research/digital-identification-and-biometrics-in-east-africa-opportunities-and-concerns/

149. Saldaña, J. (2015). The Coding Manual for Qualitative Researchers. *Sage*.

150. Sarah, C. W. (2000). Approaches to Sampling and Case Selection in Qualitative Research: Examples in the Geography of Health. *ResearchGate*.

151. Scaria, B. (2022, February 3). *The Importance of a National Digital Identity System*. Retrieved from https://www.isaca.org: https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/the-importance-of-a-national-digital-identity-system

152. Schirn, A. (2024, March 13). *ISO/IEC 27014:2020—Governance Of Information Security*. Retrieved from https://blog.ansi.org: https://blog.ansi.org/iso-iec-27014-2020-information-security-governance/

153. Scott Ainslie, D. T. (2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. *Elsevier*, 1-14.

154. Security Scientist. (2024, 04 23). *4 different Definitions of Cybersecurity from NIST*. Retrieved from https://www.securityscientist.net: https://www.securityscientist.net/blog/the-definition-of-cybersecurity-according-to-nist/

155. Showkat, N. (July 2017). In-depth Interview. *ResearchGate*.

156. Singh, P. (2022). The Importance of a National Digital Identity System. *ISACA JOURNAL, Volume 1*, 4. Retrieved from www.CANCOM.info.com.

157. Smith, A. D. (2008, September 13). *The benefits and risks of national identification programmes*. Retrieved from https://www.emeraldgrouppublishing.com: https://www.emeraldgrouppublishing.com/archived/learning/management_thinking/articles/national_id.htm

158. Soiferman, L. K. (April 2010). *Compare and Contrast Inductive and Deductive Research Approaches* . University of Manitoba.

159. STI. (October 2010). *The Federal Democratic Republic of Ethiopia National Science, Technology and Innovation Policy:Building Competitiveness through Innovation.* Addis Ababa: FDRE.

160. Swinton, S. &. (2019). Cybersecurity governance, part 1: 5 fundamental challenges. . *Carnegie Mellon University, Software Engineering Institute Insights. Retrieved June 11, 2025, from https://insights.sei.cmu.edu/blog/cybersecurity-governance-part-1-5-fundamental-challenges/*.

161. SWINTON, S., & HEDGES, S. (2019, July 25). *https://insights.sei.cmu.edu/blog/cybersecurity-governance-part-1-5-fundamental-challenges/*. Retrieved from https://insights.sei.cmu.edu.

162. Taye, T. (2023). Ethiopian National ID Program, Digital Ethiopia 2025 Strategy and Information Security.

163. Taylor, M. (2021, July 13). Retrieved from https://gds.blog.gov.uk/: https://gds.blog.gov.uk/2021/07/13/a-single-sign-on-and-digital-identity-solution-for-government/

164. Thales. (2022, August 17). *How have people proven their identity since the dawn of time?- Digital Identity*. Retrieved from https://dis-blog.thalesgroup.com: https://dis-blog.thalesgroup.com/identity-biometric-solutions/2021/06/24/how-have-people-proven-their-identity-since-the-dawn-of-time/

165. Thomas, W. E. (2017). *Research Methods for Cyber Security.*

166. Tomas, M. (2022, September 16). *Why the Ethiopian Economy Needs a National ID?* Retrieved from https://shega.co: https://shega.co/post/why-the-ethiopian-economy-needs-a-national-id/

167. Trochim, W. M. (2007). The Research Methods Knowledge Base. *ResearchGate*.

168. Trulioo. (2019, November 13). *100,000 years of identity verification: an infographic history*. Retrieved from https://www.trulioo.com: https://www.trulioo.com/blog/identity-verification/infographic-the-history-of-id-verification

169. Turner, Q. L. (2018). Identity and national identity. *Educational Philosophy and Theory, 50*(12), 1080-1088. doi:10.1080/00131857.2018.1434076

170. Tuure Tuunanen, M. R. (2007). A Contigency Model for Requirements Development. *JAIS*.

171. UNECA. (2023, June 8). *Ethiopia's Digital ID Ecosystem; Challenges, Opportunities and Lessons*. Retrieved from https://www.uneca.org: https://www.uneca.org/sites/default/files/TCND/Digital%20ID%20_in_Ethiopia.pdf

172. veriff. (2022, MAY 10). *The history of ID*. Retrieved from https://www.veriff.com: https://www.veriff.com/blog/the-history-of-id

173. Virginia, B. &. (2006). Using thematic analysis in psychology. *ResearchGate*, 77-101.

174. W R Shadish, T. D. (2002). *Experimental and Quasi-Experimental Designs for Generalized Causal Inference.* Northern University .

175. Waris Aiemworawutikul, M. V. (December 2019, june 6). *Vulnerability Assessment in National Identity Services.* doi:DOI:10.1184/R1/12431249.V1

176. Yazeed Alkhurayyif. (2015). Security Concerns with National ID Cards. *International Journal of Computing Science and Information Technology, Vol.1 (02), ISSN: 2278-9669, April 2013 (http://ijcsit.org)*, 44 - 48.

177. Yilma, K. (2022). On Ethiopia's Digital ID Bill, Data Privacy, Warts and Al. *16(2) Mizan Law Review: ,* 455-466.

178. Zahlimar, A. B. (2023). Analysis and Study of the Use of Digital National Identity Card Services in Generation Z. *Open Access Indonesia Journal of Social Sciences Vol 6 Issue 5*, 1061-1061.

Appendix 1: Interview Questions

An informed consent process was established with all interviewees, ensuring they were fully informed about the interview's purpose, question nature and the utilization of their responses. Participants had the opportunity to provide voluntary consent to partake in the interview. Confidentiality measures were upheld to protect participants' responses, ensuring that their identity and any sensitive information disclosed remain confidential and are only utilized for research purposes. Privacy was respected throughout the interview process, with interviewers avoiding intrusive questions that may infringe upon participants' privacy rights or cause discomfort. Interview questions were formulated to avoid causing harm or distress to participants, and focus on neutrality to minimize the risk of emotional or psychological harm. Transparency in the research process was maintained with participants having a clear understanding of how their data was collected, analyzed, and reported, and how their responses will contribute to the research findings. Addressing power dynamics, particularly in questions related to senior leadership oversight, involved creating a supportive and non-judgmental environment that encourages open dialogue. Finally, respect for participants' autonomy was ensured by allowing them to withdraw from the interview at any time if they felt uncomfortable or unwilling to continue, empowering them to decline to answer any questions they were not comfortable with.

1. **CS Strategy and Goal**
    1.1. Do you have a cybersecurity strategy and goal set for your organization?
    1.2. What types of security policies do you have in place in your organization?
    1.3. Do your security policies effectively address your cyber risks (identified in **risk assessments)**?
    1.4. Cybersecurity strategy should support your business; how do you measure the effectiveness of the cybersecurity strategy and goals in supporting the achievement of business objectives?

2. Senior Leadership Oversight/ Commitment

2.1. Is there a defined **governance structure** for the cybersecurity in the organization?

2.1.1. What are the roles, responsibilities, and **reporting lines** within the cybersecurity governance structure?

2.2. How is the senior leadership's commitment in providing oversight and guidance for the cybersecurity program?

2.2.1. How is the senior leadership **oversight** of

<table>
<tr><th></th><th>Yes</th><th>No</th></tr>
<tr><td>o The development and implementation of cybersecurity policies, frameworks, and guidelines? (Ensuring)</td><td></td><td></td></tr>
<tr><td>o Ensuring CS initiatives and programs achieves its intended outcomes?</td><td></td><td></td></tr>
<tr><td>o Resource Allocation (budget, personnel, and technology) for cybersecurity initiatives?
<table>
<tr><th></th><th>Yes</th><th>No</th></tr>
<tr><td>✓ Whether they are allocated in a strategic and prioritized manner?</td><td></td><td></td></tr>
<tr><td>✓ Are the resources sufficient to support the organization's cybersecurity objectives?</td><td></td><td></td></tr>
</table></td><td></td><td></td></tr>
<tr><td>o The effectiveness of risk management strategies, controls, and mitigation measures implemented under their oversight.</td><td></td><td></td></tr>
<tr><td>o The development of incident response plans, conducting drills and exercises, and ensuring timely and appropriate responses to cyber security incidents. (Approving and reviewing)</td><td></td><td></td></tr>
<tr><td>o Culture of cybersecurity awareness throughout the organization?
✓ What are their efforts in promoting cybersecurity education and training programs and ensuring that employees understand their roles and responsibilities in maintaining a secure environment?</td><td></td><td></td></tr>
</table>

3. **Standardized process**
    3.1. Does the organization use a standardized process that may include international or industry-specific standards and best practices for ensuring cybersecurity?
    3.2. What are the challenges in adhering to or following those standardized processes?
4. **Enforcement and Accountability**
    4.1. What are the legal and regulatory compliance requirements that the organization has in the cybersecurity domain?
    4.2. How does the organization ensure compliance with relevant legal and regulatory frameworks?
    4.3. How does the organization ensure that cybersecurity policies and practices align with applicable laws and regulations?
    4.4. What measures are taken to hold the organization accountable for non-compliance with legal and regulatory requirements?
5. **Resource Allocation**
    5.1. How do you prioritize the allocation of resources for cybersecurity with other organizational needs?
    5.2. Are the IT team and security professionals treated as one or differently within the organization?
    5.3. What are the challenges or factors that influence when making decisions about the allocation of resources for the cybersecurity program and initiatives?

Appendix 2: Additional Case-Scenarios

Scenario 5

Scenario 5: Mitigating a Phishing Attack Targeting the NID Program

Context:

The National Identification program becomes the target of a sophisticated phishing attack. Attackers send fraudulent emails and messages to NID program employees and registered users, attempting to trick them into revealing login credentials, sensitive data, or installing malicious software. If successful, this could lead to unauthorized access to NID systems, data breaches, and other severe consequences.

1. **Govern Phase**

Goal: Ensure strong leadership and governance to manage and mitigate the phishing attack.

- **Senior Leadership Commitment:** Leadership prioritizes the phishing incident, ensuring immediate allocation of resources and decisive actions. The incident response plan is activated under the guidance of senior management.
- **Governance Structures:** The incident response team is mobilized, with clear roles and responsibilities for detecting, managing, and mitigating the phishing attack.
- **Cybersecurity Policy and Strategy Reviews:** The cybersecurity policy is reviewed and updated to reinforce email security protocols, user awareness, and anti-phishing measures.

Outcome: A well-organized, leadership-driven response that empowers teams to address the phishing attack effectively.

2. Identify Phase

Goal: Quickly identify the phishing vectors and assess the potential impact.

- **Risk Assessment:** Conduct a comprehensive risk assessment to determine the scale of the phishing attack, identify who has been targeted, and assess any potential compromise of sensitive data.
- **Policy Enforcement:** Enforce strict email security policies, such as flagging suspicious emails and preventing access to phishing links through email filtering systems.
- **Compliance Check:** Ensure compliance with legal and regulatory requirements, including notifying affected individuals and relevant authorities about the phishing attempt.

Outcome: The phishing vectors are identified and contained, preventing further compromise.

3. Protect Phase

Goal: Implement measures to prevent further phishing attempts and secure vulnerable assets.

- **Risk Mitigation Strategies:** Deploy immediate anti-phishing defenses such as two-factor authentication (2FA), stronger password policies, and email authentication protocols (e.g., DMARC, DKIM, SPF).
- **Technology Integration:** Use advanced security tools like AI-driven email filters, sandboxing for suspicious attachments, and endpoint protection to block phishing emails and associated malware.
- **Stakeholder Engagement:** Engage with employees, partners, and users to ensure they are aware of the phishing threat and understand how to avoid falling victim to it.

Outcome: The risk of successful phishing attacks is minimized through enhanced protection measures and awareness.

4. Detect Phase

Goal: Ensure timely detection of phishing attempts and prevent unauthorized access.

- **Continuous Monitoring:** Implement real-time monitoring of email systems, network traffic, and user activity to detect phishing attempts and identify compromised accounts immediately.
- **Audit Insights:** Review email logs, network access records, and user behavior analytics to detect any signs of phishing emails or unauthorized access resulting from them.

Outcome: Phishing attempts are detected quickly, and compromised accounts are identified and secured.

5. Respond Phase

Goal: Effectively manage the phishing incident and prevent further damage.

- **Incident Management Strategy:** Activate the phishing response plan, including isolating compromised accounts, resetting passwords, and removing phishing emails from the system.
- **Communication Plan:** Execute a clear communication strategy to inform employees, stakeholders, and users about the phishing threat, providing them with guidance on recognizing phishing emails and reporting suspicious activity.
- **Reporting:** Document the incident, including actions taken and communication efforts, to ensure transparency and accountability, as well as compliance with regulatory requirements.

Outcome: The phishing attack is contained, affected users are secured, and the organization's response is well-coordinated.

6. Recover Phase

Goal: Restore normal operations, address any compromises, and improve resilience against future phishing attacks.

- **Business Continuity Planning:** Ensure that critical services are fully restored and that any data or systems impacted by the phishing attack are secured and recovered.

- **Awareness and Training:** Conduct targeted awareness and training sessions for employees and users to strengthen their ability to recognize and avoid phishing attacks in the future.
- **Post-Incident Review:** Perform a thorough review of the phishing attack, response efforts, and lessons learned to improve policies, detection, and response strategies.

Outcome: Normal operations are restored, and the organization's defense against phishing attacks is strengthened through improved training, policies, and technology.

Scenario 6

Scenario 6: Managing Insider Threats in the NID Program

Context:

An insider threat is detected within the National Identification program, where an employee with authorized access is misusing their privileges to manipulate data and share sensitive information with unauthorized parties. This poses a serious risk to the integrity and security of the NID system. The cybersecurity framework is applied to address and mitigate the impact of this insider threat effectively.

1. Govern Phase

Goal: Ensure leadership-driven governance to address and mitigate insider threats.

- **Senior Leadership Commitment:** Leadership is actively involved in addressing the insider threat, providing clear direction and allocating resources to manage and mitigate the risk.
- **Governance Structures:** Activate governance frameworks that include mechanisms to detect and respond to insider threats. Clearly define roles and responsibilities for managing insider-related incidents across various teams.
- **Cybersecurity Policy and Strategy Reviews:** Regularly review and update cybersecurity policies, focusing on access controls, employee monitoring, and data protection to mitigate insider risks.

Outcome: A leadership-driven governance structure that ensures proactive management and containment of insider threats.

2. Identify Phase

Goal: Detect and assess the scope of the insider threat to prevent further damage.

- **Risk Assessment:** Conduct a thorough risk assessment to identify the scope of the insider threat, including which systems have been compromised, the extent of data exposure, and the potential impact.
- **Policy Enforcement:** Enforce strict policies to limit access to sensitive data and systems immediately upon detection of the insider threat. Implement additional checks on activities performed by users with privileged access.
- **Compliance Check:** Ensure that the organization's response to the insider threat complies with legal and regulatory requirements, especially regarding data privacy and employee rights.

Outcome: Full identification of the insider threat, with policies enforced to contain and mitigate further risks.

3. Protect Phase

Goal: Strengthen safeguards to prevent the escalation of the insider threat.

- **Risk Mitigation Strategies:** Implement risk mitigation strategies such as revoking or limiting the insider's access, enhancing monitoring of privileged accounts, and securing all sensitive data to prevent further misuse.
- **Technology Integration:** Deploy security technologies such as Data Loss Prevention (DLP), User and Entity Behavior Analytics (UEBA), and automated monitoring tools to detect and block unauthorized activities by insiders.
- **Stakeholder Engagement:** Engage internal and external stakeholders to coordinate the response and ensure that any legal or organizational requirements are met.

Outcome: Insider access is controlled and monitored, with strengthened safeguards against further misuse of privileges.

4. Detect Phase

Goal: Ensure timely detection of insider activities and implement swift countermeasures.

- **Continuous Monitoring:** Use continuous monitoring tools to detect any suspicious behavior or activities by insiders, such as unauthorized data transfers, unusual access patterns, or attempts to bypass security controls.
- **Audit Insights:** Regularly audit system logs, access records, and employee actions to identify potential indicators of insider threats that may have been missed.

Outcome: Insider activities are detected promptly, enabling quick intervention and response to minimize damage.

5. Respond Phase

Goal: Effectively manage and neutralize the insider threat to protect the organization.

- **Incident Management Strategy:** Deploy a well-defined incident management strategy tailored to insider threats, including isolating the insider, securing compromised data, and initiating disciplinary or legal actions as necessary.
- **Communication Plan:** Execute a communication plan to inform relevant stakeholders about the insider threat, while ensuring that sensitive details are kept confidential to prevent unnecessary panic or reputational damage.
- **Reporting:** Document all actions taken during the response to the insider threat, including evidence collection, mitigation steps, and communications, to ensure transparency and compliance.

Outcome: The insider threat is neutralized, with comprehensive documentation and communication ensuring effective resolution and minimal disruption.

6. Recover Phase

Goal: Restore normal operations and reinforce defenses against future insider threats.

- **Business Continuity Planning:** Ensure that the NID program continues to function with minimal disruption during the investigation and remediation process. Implement temporary measures to maintain operations if needed.
- **Data Restoration:** Verify and restore any compromised or altered data, ensuring that the integrity of the NID database is fully restored. Use secure backups to replace any affected records.
- **Post-Incident Review:** Conduct a post-incident review to analyze the causes and impact of the insider threat. Use the insights gained to improve policies, monitoring practices, and overall resilience against insider risks.

Outcome: The NID program's integrity is restored, and the organization is better equipped to prevent and respond to future insider threats.

Scenario 7

Scenario 7: Managing Advanced Persistent Threats (APTs) in the NID Program

Context:

An Advanced Persistent Threat (APT) targets the National Identification program, attempting to gain long-term, covert access to the system to exfiltrate sensitive personal data over time. APTs are often state-sponsored and highly sophisticated, requiring a comprehensive and coordinated response. The cybersecurity framework is applied to detect, respond to, and mitigate the APT.

1. Govern Phase

Goal: Establish leadership and governance structures to manage APT risks.

- **Senior Leadership Commitment:** Senior leaders are directly involved in managing the APT, ensuring that resources are allocated, and strategic decisions are made quickly to contain the threat.
- **Governance Structures:** Activate existing governance structures designed to address sophisticated threats like APTs. Ensure that all teams involved in cybersecurity are coordinated and aware of their roles in managing the incident.
- **Cybersecurity Policy and Strategy Reviews:** Review and update cybersecurity policies and strategies with a focus on advanced threat detection, incident response, and long-term threat management.

Outcome: A well-coordinated and leadership-driven response that prepares the organization to address the complexities of APTs.

2. Identify Phase

Goal: Detect and assess the APT's presence and impact on the NID program.

- **Risk Assessment:** Conduct a thorough risk assessment to determine the extent of the APT's infiltration, including the identification of compromised systems, the data at risk, and potential vulnerabilities exploited by the attackers.
- **Policy Enforcement:** Implement and enforce strict access controls and monitoring policies to identify and isolate compromised systems and prevent further intrusion.
- **Compliance Check:** Ensure compliance with legal and regulatory requirements related to data breaches, including notification to relevant authorities if required.

Outcome: The APT's presence is fully identified, and policy enforcement helps to limit further access and damage.

3. Protect Phase

Goal: Strengthen defenses to prevent the APT from causing further harm.

- **Risk Mitigation Strategies:** Deploy immediate risk mitigation strategies such as segmenting the network, isolating critical systems, and enhancing encryption to protect sensitive data from exfiltration.
- **Technology Integration:** Integrate advanced security technologies such as Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and Threat Intelligence platforms to detect and prevent further APT activities.
- **Stakeholder Engagement:** Engage key internal and external stakeholders, including cybersecurity experts and government agencies, to coordinate a robust defense against the APT.

Outcome: Strengthened security measures and enhanced collaboration with stakeholders reduce the APT's ability to continue its activities.

4. **Detect Phase**

Goal: Ensure continuous and sophisticated detection of the APT's activities.

- **Continuous Monitoring:** Deploy continuous monitoring tools capable of detecting advanced threats, such as APTs, which often evade traditional detection mechanisms. Use behavior-based detection to identify anomalies indicative of an APT.
- **Audit Insights:** Regularly review and analyze audit logs, historical data, and system behaviors to detect any signs of ongoing APT activity that may have previously gone unnoticed.

Outcome: The APT's activities are continuously monitored, allowing for early detection of any attempts to escalate the attack.

5. **Respond Phase**

Goal: Execute a coordinated response to neutralize the APT and minimize damage.

- **Incident Management Strategy:** Deploy a comprehensive incident management strategy specifically tailored for APTs, including containment, eradication, and remediation steps. Work with specialized teams to develop countermeasures.
- **Communication Plan:** Implement a secure communication plan to ensure that all stakeholders are informed without alerting the attackers, maintaining the confidentiality of response actions.
- **Reporting:** Document all actions taken during the response, ensuring that evidence is preserved for potential legal action and future analysis.

Outcome: The APT is contained and neutralized, with minimal impact on operations, and the response actions are well-documented.

6. Recover Phase

Goal: Restore normal operations while enhancing resilience against future APTs.

- **Business Continuity Planning:** Ensure that business continuity plans are executed to minimize operational disruption during the response and recovery phases. Implement interim measures to keep critical functions running.
- **Data Restoration:** Carefully restore data from secure backups, ensuring that any data compromised or altered by the APT is fully recovered without reintegrating malicious elements.
- **Post-Incident Review:** Conduct an in-depth post-incident review to understand how the APT infiltrated the system, identify weaknesses, and apply lessons learned to improve future defense mechanisms.

Outcome: The NID program's operations are fully restored, and the organization is better prepared to detect, respond to, and recover from future APTs.