

UNIVERSITY OF BAHRAIN

**College of Information
Technology**

**Department of
Computer Engineering**



Cybersecurity Governance Framework to Mitigate Cyberattacks: A Case Study in Saudi Arabia

A Thesis Submitted in Partial Fulfillment of the Requirements for the
Master of Science in Cybersecurity

Submitted By

Arwa Alromaih

20190266

Supervised By

Dr. Mazen Ali

(Associate Professor)

University of Bahrain

November 2024



Dissertation Deposit Form

Author Name:	Arwa Mohammed Alromaih		
Email:	20190266@stu.uob.edu.bh	Contact No:	Click here to enter text.
College:	Information Technology		
Department:	Computer Engineering		
Thesis Title:	Cybersecurity Governance Framework to Mitigate Cyberattacks: A Case Study in Saudi Arabia		
Year:	2024		

Author's Declaration: I agree to the following conditions:

The above thesis will be available (in the University of Bahrain library and externally) and reproduced as necessary at the discretion of the University of Bahrain. It may also be digitized by the University of Bahrain and made available via the university's repository or via other parties on the Internet.

This condition shall apply to ALL copies including electronic copies.

The above thesis has been provided on the understanding that it is copyright protected material and that no quotation from this thesis may be published without proper acknowledgement.

Signature of the Author:	Arwa Mohammed Alromaih	Date:	14-May-24
--------------------------	------------------------	-------	-----------

ABSTRACT

The increasing frequency and sophistication of cyber threats, especially targeting national critical infrastructure, highlight the urgent need for an effective cybersecurity governance framework. This research addresses a significant gap in understanding and implementing cybersecurity governance designed specifically for critical infrastructure within Saudi Arabia, a sector facing heightened vulnerability to complex cyber risks. Employing a comprehensive case study approach, this study integrates the Capability Maturity Model Integration (CMMI) V1.3 with leading frameworks—NIST CSF v1.1, COBIT 2019, and SABSA. Data collection from 2022 to 2024 provides a thorough assessment of the maturity, capability, and resilience of cybersecurity governance within a critical infrastructure organization.

Using a structured, five-phase EGIT (Enterprise Governance of Information and Technology) program, this methodology rigorously evaluates and enhances cybersecurity governance. CMMI V1.3 measurement techniques assess maturity levels across cybersecurity controls, enabling each business unit to perform self-assessments and refine objectives based on capability and maturity. Through the integration of time-based strategies and customized governance tools, the study demonstrates a notable maturity progression from level 1.3 to 2.7 within a year, reflecting significant improvement in the organization's resilience.

Key findings reveal the practical impact of cybersecurity governance on protecting critical infrastructure, achieved by implementing governance frameworks specifically adapted to the Saudi context. The study's unique approach integrates COBIT, NIST CSF, and SABSA within a coherent framework tailored to national regulations—offers new insights into the benefits of combining established governance models with region-specific needs. The proposed continuous improvement model, including CMMI maturity assessments and periodic threat evaluations, promotes sustained resilience as the threat landscape evolves. This research not only advances the theoretical framework of cybersecurity governance but also provides actionable recommendations for critical infrastructure organizations in Saudi Arabia, aligning with the Kingdom's Vision 2030 objectives for a robust and secure digital economy.

Contents

APPROVAL	A
ABSTRACT	B
TABLE OF CONTENTS	C
LIST OF FIGURES	H
LIST OF TABLES	I
ACKNOWLEDGMENTS	J
DEDICATION	K
LIST OF ABBREVIATIONS	L
1 Introduction	1
1.1 Overview	1
1.2 Research Problem	5
1.3 Research Questions	7
1.4 Research Objectives	7
1.5 Research Significance	9
1.6 The Study's Setting	10
1.7 Research Terminology	11
1.8 Thesis Outline	14
2 Literature Review	16
2.1 Literature Review	16
2.1.1 Introduction	16
2.1.2 Most Common Types Of Cyber Attacks	18
2.1.3 Mechanisms to Deter Cyberattacks	33

2.1.3.1	Malware	33
2.1.3.2	System Compromise	34
2.1.3.3	Denial of Service (DoS)	35
2.1.3.4	Personal/Sensitive Data Breach	35
2.1.3.5	Social Media Attacks	36
2.1.3.6	Phishing Attacks	37
2.1.3.7	Insider Attacks	37
2.1.3.8	Website Hacks	38
2.1.4	Assessment of COBIT 2019, NIST CSF v1. 1, and SABSA Frameworks	39
2.1.5	Building a Cybersecurity Governance Framework .	40
2.1.6	Assessments of COBIT 2019 Practices	41
2.1.7	NIST CSF v1. 1 Assessment	54
2.1.8	SABSA Architecture Matrix Assessment	58
2.1.9	Maturity and Capability Measurement using CMMI V2.0 Methodology	60
2.1.9.1	Integration with Other Frameworks	61
2.1.9.2	Security and Defense in Depth	62
2.1.9.3	Continuous Improvement in Cybersecurity Governance	63
2.1.10	Identification of Key Gaps and Concerns	64
2.1.11	Conclusion	67
3	Research Method	68
3.1	Research Method	68
3.2	Methodology Used	69
3.2.1	Research Purpose and Strategy	69
3.2.1.1	Research Approach	69
3.2.1.2	Research Strategy	70
3.2.2	Data Collection	70

3.2.2.1	Primary Data Collection	70
3.2.2.2	Secondary Data Collection	71
3.2.2.3	Participant Selection Criteria	71
3.2.3	Data Analysis	71
3.2.3.1	Qualitative Data Analysis	72
3.2.3.2	Quantitative Data Analysis	72
3.2.4	Research Tools	73
3.2.4.1	RACI Matrix and COBIT 2019	73
3.2.4.2	COBIT 2019 Governance and Management Objectives, Practices, and Activities	75
3.2.4.3	COBIT 2019 Governance System Design Toolkit	77
3.2.4.4	Cybersecurity Governance Tool	81
3.2.5	Conclusion	86
4	Case Study Analysis	87
4.1	Case Study Analysis	87
4.2	Case Study	88
4.2.1	Organization Alpha	88
4.2.2	Business Challenges	88
4.2.3	Data Collection Design	90
4.2.4	Assessment Findings	91
4.2.5	Current Cybersecurity Maturity and Incident Response	93
4.2.5.1	Cybersecurity Control Assessment Process	94
4.2.5.2	Incident Response Procedures for Com- mon Cyberattacks (2020-2021)	96
4.2.5.3	Analysis of Incident Response	100
4.2.6	Quantitative Cybersecurity Risks and Their Impact	101
4.2.6.1	Key Cybersecurity Risks Identified	101
4.2.6.2	Analysis of the Risk Data	102

4.2.7	EGIT Program Implementation	103
4.2.8	Scope Definition and Expansion	103
4.2.9	Significance of EGIT Program Outcomes	103
4.2.10	Strategic Approach and Stakeholder Engagement . .	103
4.2.11	Enhancing IT Process Capability	104
4.2.12	Capability and Maturity Assessment	104
4.2.13	Five Sequential Phases Approach	104
4.2.14	Challenges and Stakeholder Approval	105
4.2.15	First Phase: Comprehensive Action Plan for EGIT Program Implementation	105
4.2.16	Second Phase: Design of EGIT Program Implemen- tation	108
4.2.17	Third and Fourth Phases Program Implementation and Assessment:	111
4.2.18	Fifth Phase Monitoring and Enhancement:	113
4.2.19	Cybersecurity Governance Tool:	114
5	Results, Discussion, and Recommendations	119
5.1	Results, Discussion, And Recommendations	119
5.1.1	The Study's Results	119
5.1.1.1	Analysis of Incident Response	123
5.1.1.2	Quantitative Cybersecurity Risk Assess- ment and Analysis	123
5.1.1.3	Risk Metrics Overview	124
5.1.1.4	Risk Assessment Matrix	124
5.1.1.5	Cost-Benefit Analysis	126
5.1.1.6	Incident Response Times	126
5.1.1.7	Number of Incidents Before and After Frame- work Implementation	126
5.1.1.8	Results of the Research Questions	127

5.2	Discussion of Results	134
5.2.1	Contribution to Cybersecurity Governance Frame- works	134
5.2.2	Time-Based Cybersecurity Approach and Defense Strategies	135
5.2.3	Effectiveness of Practical Solutions	135
5.2.4	Implications for Cybersecurity in Critical Infrastruc- ture	136
5.3	Contribution to the Field	136
5.4	Study's Recommendations	138
5.5	Limitations of the Study and Future Considerations	140
5.5.1	Limitations of the Study	140
5.5.2	Future Considerations	141
5.6	Conclusion	142
	Abstract (in Arabic)	144
	Appendix	146
	Interview Logs	146
	PUBLICATIONS	155
	References	156

List of Figures

4.1 Selected enterprise and alignment goals and metrics referring to the COBIT® 2019 Framework: Governance and Management Objectives. 108

List of Tables

5.2 Comparison of NIST CSF v1. 1, COBIT 2019, and SABSA
frameworks in the context of various cyber attack types. . . . 129

5.3 Conducted Workshops Details 150

ACKNOWLEDGMENTS

I am deeply grateful to my husband and family for their unwavering love, encouragement, and understanding throughout this academic journey. Your support has been my rock, inspiring me to reach for excellence.

I extend my sincere appreciation to my supervisor, Dr. Mazen Ali, for his exceptional guidance, wisdom, and patience. His mentorship has been instrumental in shaping my research and academic growth.

I am also thankful to my instructor, Dr. Wael Elmedany, for his valuable insights, support, and expertise, which have enriched this thesis.

To everyone who has contributed to my success, whether through encouragement, feedback, or assistance, thank you for being a part of this significant milestone in my life.

DEDICATION

Dedicated to my beloved husband for his unwavering support and encouragement.

LIST OF ABBREVIATIONS

NIST CSF v1.1	National Institute of Standards and Technology Cybersecurity Framework
COBIT	Control Objectives for Information and Related Technologies
SABSA	Sherwood Applied Business Security Architecture
CMMI	Capability Maturity Model Integration
EGIT	Enterprise Governance of Information Technology
KPI	Key Performance Indicators
RACI	Responsible, Accountable, Consulted, Informed

Chapter 1

Introduction

1.1 Overview

In a time of increasing dependence on the digital world, the crucial significance of cybersecurity has emerged as a crucial concern for nations across the globe. Cyber threats that pose significant risks to governments, businesses, and individuals continue to evolve as information technology continues to evolve. According to the National Cybersecurity Authority (NCA) in Saudi Arabia, the Shamoon malware impacted several critical infrastructures in 2012 and caused significant damage. It returned in 2016 and spread across more private and government sectors, resulting in even greater damage and elevating the risk to catastrophic levels (*Securing the Grid*, 2020). From 2020 to 2024, the financial impact of cybercrime has shown a dramatic increase. In 2022 alone, identity fraud resulted in losses amounting to \$20 billion, affecting 15.4 million U.S. adults, according to Javelin Strategy & Research's "2023 Identity Fraud Study: The Butterfly Effect" (Kerner, 2022). Additionally, the FBI's Internet Crime Complaint Center reported that total losses from cybercrime complaints in 2023 reached \$12.5 billion, a 10% increase from the previous year (Kerner, 2022). Looking ahead, the annual average cost of cybercrime is projected to escalate significantly, expected to reach more than \$23 trillion by 2027, up from \$8.4 trillion in 2022,

as highlighted by Anne Neuberger, U.S. Deputy National Security Advisor for cyber and emerging technologies (Kerner, 2022). These findings are further supported by Sean Michael Kerner's comprehensive report on cybersecurity statistics (Kerner, 2022). Moreover, the SolarWinds breach in 2020 and the Colonial Pipeline ransomware attack in 2021 further underscore the persistent and evolving nature of cyber threats, emphasizing the urgent need for robust cybersecurity measures and governance structures to mitigate risks (Greiman, 2023). These incidents highlight the importance of taking a comprehensive approach to cybersecurity governance to safeguard critical infrastructure worldwide (Alashi & Badi, 2020).

Since the COVID-19 lockdown, teleworking has become common in many organizations worldwide. Employees now have the flexibility to work remotely on a part-time or permanent basis. This transition has resulted in a reduction of traditional security measures (e.g., CCTV, locked doors, security guards) and logical security controls (e.g., software updates). The use of insecure Wi-Fi networks further compromises sensitive information. Consequently, these factors weaken cybersecurity defenses, heightening the risk of cyber attacks such as phishing, ransomware, and financial fraud (Alromaih, Abdulwahab, & Zeki, 2021). Additionally, attackers employ social engineering techniques that exploit human emotions like fear and urgency. For instance, they may impersonate financial or HR department personnel, request information under the appearance of payroll processing, or pose as IT security staff asking for a One-Time Password (OTP) to unlock an account. These vulnerabilities provide attackers with numerous opportunities to breach organizational defenses, potentially causing significant damage. Moreover, the new war strategy has evolved into a hybrid approach that relies heavily on cyberattacks, which are less costly and more effective in targeting a country's critical infrastructure. This was evident in the significant impact on Ukraine's critical infrastructure, affecting multiple sectors

(Simons, Danyk, & Maliarchuk, 2020).

Effective cybersecurity governance is crucial in preventing, detecting, and responding to cyber-attacks as it establishes a structured approach to risk management and resilience (of Standards & Technology, 2018). The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF v1. 1) emphasizes the importance of a proactive strategy to identify and mitigate cyber threats (of Standards & Technology, 2018). Governance frameworks provide a foundation for implementing robust controls, ensuring continuous monitoring, and fostering a culture of cybersecurity awareness, which collectively enhance an organization's ability to prevent and detect attacks (International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), 2013). A well-defined governance framework also facilitates swift and coordinated response efforts, minimizing the impact of online threats on corporate assets and operations (Setiadi & Fianty, 2024). Organizations have used different ways to protect themselves online, like adopting NIST CSF v1. 1, or COBIT, or ISO/IEC 27001, but they still get attacked by hackers (Savaş & Karataş, 2022).

It is imperative to acknowledge that cybersecurity is undergoing continuous evolution and that it is imperative to establish a dynamic Cybersecurity governance to remain abreast of the latest developments (*COBIT 2019 Framework*, 2018). Even though cybersecurity governance is not a novel concept in the realm of IT, there are a few established studies pertaining to it. One of the studies found on cybersecurity governance to ensure cybersecurity presents a comprehensive examination of the concept and practice of cybersecurity governance (Savaş & Karataş, 2022). The research provides oversight to ensure efficient risk mitigation and proposes a framework for cyber governance based on four dimensions: normative, institutional, technical, and strategic. The study examines cyber governance in legal, po-

litical, social, and technical contexts, focusing on the online environment and dividing it into public and private sectors and individuals to recommend the need for an international cybersecurity governance framework (Savaş & Karataş, 2022).

Nonetheless, the authors failed to investigate the correlation between cybersecurity governance and cyberattacks to mitigate the harm done to the organization's assets. The second research found within cybersecurity governance failed to study the role of cybersecurity governance, which focused on business corporations (Saha & Anwar, 2024). The study emphasizes the critical role of cybersecurity governance in addressing challenges like strategy, unified processes, and accountability (Awan & Pitafi, 2024).

Furthermore, the risks from industrial espionage underscore the need for strategic cybersecurity planning. Also, the need for cybersecurity governance that involves senior leadership contributes to sustainable cybersecurity (Alashi & Badi, 2020). However, the research lacks an analysis of the relationship between cybersecurity governance and cyberattacks, as well as how cybersecurity governance effectively reduces cyber threats.

These studies examined cybersecurity governance from different angles to analyze the vital role of cybersecurity governance in achieving a strong cybersecurity posture (Valavanis, 2024). While these research papers provide essential insight into cybersecurity governance, they appear to lack a detailed exploration of how these measures contribute comprehensively to reducing cyberattacks. A more in-depth analysis of the specific mechanisms within cybersecurity governance that effectively mitigate and prevent cyber threats is required to be researched. This could include insights into how the outlined steps translate into tangible improvements in cybersecurity posture, incident prevention, and overall readiness against cyberattacks (Hasan, Ali, Kurnia, & Thurasamy, 2021).

1.2 Research Problem

In the contemporary era, the relentless digitization of national critical infrastructure intensifies its susceptibility to sophisticated cyber threats, resulting in substantial economic losses on a global scale (Potter & Stilinski, 2024). Cybercrime has resulted in significant economic losses globally. In 2021, the estimated cost of cybercrime reached approximately 6 trillion dollars, which is double the 3 trillion dollars reported in 2015. Projections indicate that these losses could escalate to 10.5 trillion dollars annually by 2025 (Hawdon, 2021a). However, amid this escalating threat landscape and substantial financial ramifications, a considerable research gap persists. Existing studies highlight a deficiency in examining cybersecurity issues in critical national infrastructure, specifically from a cybersecurity governance perspective.

This research acknowledges the imperative to address this gap, offering a nuanced exploration into the impact of cybersecurity governance on safeguarding critical national infrastructure. By incorporating a recommended cybersecurity governance tool, designed for practical implementation, tracking cybersecurity maturity and capability levels, and leveraging the Capability Maturity Model Integration V1.3 (CMMI) for a dynamic approach—meaning a flexible and adaptive strategy that evolves alongside emerging threats and technological advancements—this study contributes significantly to the discourse on securing critical infrastructure in the face of evolving cyber threats.

The existing academic and research gap in cybersecurity governance frameworks aimed at mitigating cyberattacks, particularly within the context of critical infrastructure in Saudi Arabia, has not been adequately addressed. One of the primary gaps is the lack of comprehensive research in this domain, specifically targeting the unique challenges and requirements of critical infrastructure organizations in Saudi Arabia. To bridge these gaps, this study investigates the impact of cybersecurity governance in Saudi Ara-

bia.

The central research question guiding this inquiry is:

How can a tailored cybersecurity governance framework be effectively constructed and implemented within critical infrastructure organizations to enhance their cybersecurity posture?

This overarching question is further delineated into three specific sub-questions:

- In what ways does organizational cybersecurity governance influence the mitigation of cyber threats?
- What mechanisms can be employed to deter cyber-attacks in a temporal context (before, during, and after the attacks)?
- How can the proposed solutions mitigate the damage caused by various types of cyber-attacks, including Malware, System Compromise, Denial of Service, Personal/Sensitive Data Breach, Social Media Attacks, Phishing Attacks, Insider Attacks, and Website Hacks?

To answer these questions comprehensively, this study employs a structured methodology that integrates three robust frameworks – COBIT 2019, NIST CSF v1. 1, and SABSA – at the enterprise level. These frameworks, designed to align cybersecurity practices with business objectives, will be supplemented by a customized cybersecurity governance tool developed specifically for this study. Furthermore, the study acknowledges the importance of maintaining flexibility and adaptability in cybersecurity governance and will utilize the Capability Maturity Model Integration V1.3 (CMMI) to assess the maturity and capability of the selected case study. This multifaceted approach ensures a thorough examination of organizational cybersecurity governance.

The research will focus on a case study conducted within critical infrastructure in Saudi Arabia, providing invaluable insights into the practical

effectiveness of the proposed cybersecurity governance framework. This approach not only advances the discourse on organizational cybersecurity governance but also offers a tangible and adaptable solution poised for real-world application.

1.3 Research Questions

The central research question guiding this study is:

How can a tailored cybersecurity governance framework be effectively constructed and implemented within critical infrastructure organizations to enhance their cybersecurity posture?

This main question is further delineated into three specific sub-questions:

- In what ways does organizational cybersecurity governance influence the mitigation of cyber threats?
- What mechanisms can be employed to deter cyber-attacks in a temporal context (before, during, and after the attacks)?
- How can the proposed solutions mitigate the damage caused by various types of cyber-attacks, including Malware, System Compromise, Denial of Service, Personal/Sensitive Data Breach, Social Media Attacks, Phishing Attacks, Insider Attacks, and Website Hacks?

1.4 Research Objectives

In the pursuit of strengthening cybersecurity governance within the critical infrastructure of Saudi Arabia, this research introduces a dynamic and comprehensive approach. By utilizing a customized cybersecurity governance tool, integrating NIST CSF v1. 1, COBIT 2019, SABSA, and the Capability Maturity Model Integration V1.3 (CMMI), the study aims to explore the

intricate facets of organizational practices and their impact on cyber threat resilience. The research objectives are carefully structured to provide a tailored framework for each organization's needs, integrating insights from these frameworks and the governance tool, which includes a cyber risk register and KPI monitoring for the main cybersecurity domains. The key highlights of these research objectives include:

Research Aim: To develop and implement a tailored cybersecurity governance framework that significantly enhances the cybersecurity posture of critical infrastructure organizations in Saudi Arabia.

Research Objectives:

- **Objective 1: Impact Evaluation** To assess the efficacy of organizational cybersecurity governance practices in influencing the mitigation of cyber threats.
- **Objective 2: Time-Based Approach Examination** To investigate the practicality and efficiency of time-based cybersecurity strategies, particularly before, during, and after a cyber-attack, and to propose recommendations for an enhanced approach.
- **Objective 3: Solutions' Effectiveness Analysis** To evaluate the effectiveness of proposed solutions in mitigating the damage caused by various types of cyberattacks, including Malware, System Compromise, Denial of Service, Personal/Sensitive Data Breach, Social Media Attacks, Phishing Attacks, Insider Attacks, and Website Hacks.

These objectives will be informed by the cybersecurity governance tool, integrating NIST CSF v1. 1, COBIT 2019, SABSA, and CMMI V2.0, along with the cyber risk register and KPI monitoring for the main cybersecurity domains.

In conclusion, these research objectives aim to contribute substantive theoretical insights and provide practical recommendations for enhancing

cybersecurity postures, addressing the complex challenges faced by critical infrastructure in Saudi Arabia. This holistic perspective is envisioned to offer significant contributions to the evolving landscape of cybersecurity governance.

1.5 Research Significance

The significance of this research study lies in its practical benefits and the unexplored terrain it ventures into within the realm of cybersecurity governance. In an era where the digitization of critical infrastructure exposes vulnerabilities to escalating cyber threats, this study offers a dynamic approach through the integration of a cybersecurity governance tool, CMMI V2.0, and the comprehensive examination of three foundational frameworks: COBIT 2019, NIST CSF v1. 1, and SABSA.

The customized governance tool, complemented by CMMI V2.0, provides a real-time snapshot of organizational practices, enhancing the assessment of cybersecurity posture (Degerli, 2020). Moreover, the incorporation of CMMI V2.0 adds a layer of dynamism, ensuring a continuous evaluation of maturity and capability levels and addressing the ever-evolving cyber landscape (*COBIT 2019 Framework*, 2018). The inclusion of three influential frameworks enriches the research by offering a structured approach to cybersecurity governance at the enterprise level.

The research topic, centered around the impact of cybersecurity governance on critical infrastructure in Saudi Arabia, is particularly significant as it is a relatively unexplored domain. While cybersecurity governance is acknowledged as crucial, few studies investigate into its comprehensive examination within the specific context of critical infrastructure (Cantelmi, Di Gravio, & Patriarca, 2021). This research aims to bridge this gap by offering a comprehensive understanding of the relationship between orga-

nizational cybersecurity governance practices and resilience against cyber threats.

Furthermore, the pressing need for replicating the study stems from the rapid evolution of cybersecurity challenges (Hawdon, 2021b). Unlike studies conducted long ago, the contemporary landscape witnesses sophisticated cyber threats that demand an adaptive and proactive governance approach. By revisiting and advancing the study, this research provides insights into the changes that have occurred in the cybersecurity domain, offering practical recommendations to help safeguard critical infrastructure against modern cyberattacks. The anticipated benefits include a refined understanding of the effectiveness of cybersecurity frameworks, strategic insights for enhancing time-based cybersecurity approaches, and practical recommendations for organizations aiming to bolster their cybersecurity postures.

1.6 The Study's Setting

The setting for this study is the critical infrastructure landscape of Saudi Arabia, a dynamic and evolving environment marked by increased digitization and growing susceptibility to cyber threats. In recent years, the Kingdom has witnessed significant developments in its critical infrastructure systems, with sectors such as energy, water, and transportation undergoing substantial digital transformation. The topical standpoint revolves around the contemporary challenges faced by organizations in safeguarding their critical infrastructure from cyber threats. Saudi Arabia's critical infrastructure serves as the backdrop for this study due to its strategic importance and the limited research conducted in this specific context. The study setting is characterized by a heightened need for robust cybersecurity governance, given the escalating sophistication of cyber threats globally. The country has experienced cyber incidents, such as the Shamoon malware attacks, highlighting

the urgency to address cybersecurity challenges.

The study's focus on critical infrastructure in Saudi Arabia is significant, considering the economic and social implications of potential cyberattacks. The setting reflects the current landscape where organizations are grappling with the need to adopt effective cybersecurity measures to ensure the resilience of their critical infrastructure systems. The study aims to contribute insights that are particularly relevant to this setting, offering practical recommendations for enhancing cybersecurity governance tailored to the unique challenges faced by organizations in Saudi Arabia's critical infrastructure sector.

1.7 Research Terminology

It is imperative to establish a common understanding of key concepts when defining the main terms crucial to this study. The following terms are central to the research, with their respective definers and sources, and are conceptually classified based on their relevance to the focus on cybersecurity governance frameworks and practices within the specific context of Saudi Arabia's critical infrastructure.

- **Cybersecurity Governance:** Cybersecurity governance refers to the systematic approach organizations adopt to manage and oversee their cybersecurity strategies, policies, and practices (of Standards & Technology, 2018). It is the framework through which organizations ensure that cybersecurity is aligned with their business objectives, meets regulatory requirements, and provides effective risk management. Effective cybersecurity governance ensures that accountability, roles, and responsibilities are well-defined at all levels of the organization, from executive leadership to IT operations. It also involves ensuring that cybersecurity policies and procedures are regularly updated

and that the organization is resilient to emerging cyber threats. In this study, cybersecurity governance plays a crucial role in how organizations within Saudi Arabia's critical infrastructure manage their cybersecurity risk profiles and respond to cyber incidents.

- **NIST CSF v1. 1 (National Institute of Standards and Technology Cybersecurity Framework):** The NIST Cybersecurity Framework (CSF) is a set of guidelines, standards, and best practices designed to help organizations manage cybersecurity risks (of Standards & Technology, 2018). It was developed by the U.S. National Institute of Standards and Technology in response to an executive order aimed at improving the security of critical infrastructure. The framework is composed of five core functions—Identify, Protect, Detect, Respond, and Recover—allowing organizations to tailor these to their specific risk management needs. The NIST CSF v1. 1 emphasizes a risk-based approach to cybersecurity, and its flexible, scalable nature makes it suitable for organizations of all sizes and sectors, including the critical infrastructure industries in Saudi Arabia. The framework is also widely recognized internationally, making it a vital component of this study's examination of cybersecurity governance.
- **COBIT 2019 (Control Objectives for Information and Related Technologies):** COBIT 2019 is an enterprise IT governance and management framework developed by ISACA that provides a comprehensive approach to managing and governing information technology within organizations (*COBIT 2019 Framework*, 2018). COBIT 2019 focuses on ensuring that IT is aligned with business goals, delivers value, and supports enterprise risk management. It consists of a set of control objectives, management guidelines, and maturity models that help organizations achieve effective governance of IT assets, in-

cluding cybersecurity. For the purpose of this study, COBIT 2019 is central to analyzing how governance mechanisms ensure proper oversight of cybersecurity practices within Saudi Arabia's critical infrastructure. COBIT 2019 allows organizations to assess their cybersecurity governance maturity and identify gaps in their current practices.

- **SABSA (Sherwood Applied Business Security Architecture) Framework:** The SABSA Framework is a business-driven security architecture framework that aligns security strategies with the overarching business objectives of an organization (Sherwood, Clark, & Lynas, 2005). It is a risk-driven approach that focuses on security services being delivered in a way that addresses real business risks, with security architecture layered in accordance with the operational and strategic needs of the business. The SABSA matrix serves as a comprehensive model to define security architectures by focusing on six layers: business requirements, risk management, security services, logical security, physical security, and technology solutions. In this study, SABSA is critical to understanding how organizations within Saudi Arabia's critical infrastructure align their cybersecurity initiatives with broader business goals while managing and mitigating risk.
- **CMMI V2.0 (Capability Maturity Model Integration):** CMMI V2.0 is a process-level improvement training and appraisal program that provides organizations with essential elements of effective processes, including cybersecurity governance (*CMMI Version 2.0*, 2018). It enables organizations to evaluate their current process maturity, identify gaps, and implement improvements systematically. CMMI is often used to assess the maturity of cybersecurity programs, helping organizations advance from ad-hoc and reactive processes to more mature, consistent, and proactive processes. In the context of this study,

CMMI V2.0 is utilized to assess the maturity of the cybersecurity governance frameworks in use at Organization Alpha. By measuring the organization's maturity before and after the implementation of COBIT 2019, NIST CSF v1. 1, and SABSA, CMMI V2.0 provides a structured methodology to assess the progress and identify further areas for improvement.

These definitions are integral to understanding the cybersecurity governance frameworks and practices analyzed in this study. The combination of these frameworks and models provides a holistic approach to managing cybersecurity risks, enhancing the maturity of cybersecurity governance, and ensuring alignment between cybersecurity strategies and business objectives within Saudi Arabia's critical infrastructure.

1.8 Thesis Outline

The thesis is structured into several chapters to comprehensively explore the cybersecurity governance framework's implications for mitigating cyber threats within critical infrastructure.

The first chapter serves as an introduction to the study, providing an overview of the research topic's significance and the key challenges it addresses. It also outlines the specific research questions guiding the study, along with the objectives aimed at achieving through the research. Additionally, the chapter discusses the importance and potential impact of the research findings, describes the study's setting, and clarifies key terms and concepts used throughout the thesis.

The second chapter focuses on the literature review, which surveys existing literature related to cybersecurity governance frameworks and cyber threats. It covers various aspects such as mechanisms to deter cyberattacks, malware, denial of service attacks, data breaches, social media at-

tacks, phishing attacks, insider threats, website hacks, mapping of NIST CSF v1. 1, SABSA, and COBIT 2019 frameworks, building a cybersecurity governance framework, assessments of COBIT 2019 practices, NIST CSF v1. 1 assessment, SABSA architecture matrix assessment, maturity and capability measurement using CMMI V2.0 methodology, identification of key gaps and concerns, and concludes with a synthesis of the literature review.

In the third chapter, the methods and procedures employed in the research are detailed. This includes the methodology used for data collection, analysis, interpretation, and the research tools employed throughout the study.

Chapter four investigate into the case study conducted as part of the research, along with the development and application of a cybersecurity governance tool. The case study introduces the organization under study, its challenges, data collection design, assessment findings, EGIT program implementation, scope definition, strategic approach, capability and maturity assessment, detailed action plans, methodology for tool development, its application in the case study, tool effectiveness, practical implications, and recommendations based on insights from the case study and tool analysis.

The final chapter, chapter five, presents the results of the study, discusses their implications, and offers recommendations for future considerations. It covers the study's results, discussion of results, study recommendations, limitations, future considerations, and concludes with a summary of the chapter's findings.

Chapter 2

Literature Review

2.1 Literature Review

The aim of this chapter is to research and analyze what has been done in this thesis research field from 2000 until 2024. A debate will be utilized to view all the existing research online.

2.1.1 Introduction

Now more than ever, cybersecurity professionals are needed to prevent and deter attacks as they are initiated. This has highlighted the need for individuals, governments, and organizations to seek measures to reduce cyber-attacks. Information security may be likened to a health initiative - both individual and global - and governments must plan for relief, protection, and prevention strategies to ensure their information is safe (AlDaajeh & Alrabae, 2024).

This has led to an era in which it is the prime target for all entities. During a time of fast-paced worldwide integration facilitated by extensive information usage, safeguarding information has emerged as a crucial objective for all establishments. The swift advancements in technology, coupled with the remarkable capabilities and impact of the internet and cyberspace, present numerous prospects but also amplify the worldwide peril to information systems entities. In an era of rapid global integration through the widespread use of information, information security has become a critical mission for all organizations. As virtual space is unlimited, so are its borders and entities wishing to cause harm. The rate of technology and the efficiency and effectiveness of the internet and cyberspace provide many opportunities but also increase the global threat to information systems (Melaku, 2023).

The objective of information security governance is to provide direction and ensure that the information security program aligns with business objectives. In simple terms, it's the display of what can be done and what cannot be done in a fashion that does not undermine the best interest of any entity. Any violations of these laws would be equivalent to a digital steal, pilfering, or any activity that would damage another's entity in the physical world (Demirkan, Demirkan, & McKee, 2020).

Similarly, laws and regulations have taken the shape of governance in cybersecurity to rule the cyber world. Cybersecurity governance is the process of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately, and verifying that resources are used responsibly to protect the cyber environment. This includes the development of policies and oversight on how information technologies are to be used (Melaku, 2023).

2.1.2 Most Common Types Of Cyber Attacks

The accelerating growth of cyber threats targeting critical infrastructure significantly increases the risks to sensitive systems and data. Among the most prevalent cyberattacks aimed at critical infrastructure are Malware, System Compromise, Denial of Service (DoS) Attacks, Personal and Sensitive Data Breaches, Social Media Attacks, Phishing Attacks, Insider Threats, and Website Attacks. According to (George, Baskar, & Srikaanth, 2024), the vulnerability of critical infrastructure has escalated due to its increased exposure through digital transformation, the adoption of Industrial Control Systems (ICS), and the integration of the Internet of Things (IoT).

(George, Baskar, and Srikaanth, 2024) propose a comprehensive framework, suggesting the adoption of the NIST Cybersecurity Framework (NIST CSF v1. 1) as a strategic approach. However, while the NIST CSF v1. 1 is a valuable tool for managing cyber risks within complex IT environments, it may not be the ultimate solution for all critical infrastructure scenarios. In my view, while the NIST CSF v1. 1 provides a robust foundation for cybersecurity risk management, a more holistic approach is necessary. This should include a governance framework such as COBIT 2019, which embeds cybersecurity across all organizational entities, ensuring that cybersecurity measures are implemented and tailored to the organization's specific needs. Additionally, frameworks like SABSA can be instrumental in customizing cybersecurity strategies to align with organizational requirements.

Below is a list of some of the most common types of cyberattacks that this thesis will focus on:

- **Malware:** Malware often aims to alter a system's state to benefit the attacker, whether by stealing information or utilizing system resources for further malicious activities. Understanding a system's state is crucial, as it encompasses all data and conditions at a given time. Sophisticated malware can covertly control multiple systems, forming

botnets for extensive malicious activities. Malware can manifest in various forms, such as ransomware, worms, viruses, spyware, adware, rootkits, Trojan horses, etc. The impact of each type of malware varies depending on its specific characteristics and method of attack (Lee, 2024). In Saudi Arabia, two of the most significant malware incidents involved the Shamoon and Mamba ransomware attacks, severely affecting the country's critical infrastructure. Shamoon, a data-wiping malware, first emerged in 2012 and targeted one of the world's largest oil and gas companies. The attackers successfully embedded the Shamoon malware code within a Word document, activated upon opening the file. The same malware reappeared in 2016 as Shamoon 2, targeting multiple organizations within Saudi Arabia's critical infrastructure. On the other hand, Mamba ransomware was designed to infiltrate organizations, encrypting their data and holding it hostage until a ransom was paid (Al-Mulhim, Al-Zamil, & Al-Dossary, 2020).

The paper by (Al-Mulhim, Al-Zamil, and Al-Dossary, 2020) analyzes these two malware incidents, discussing their methodologies, histories, and significant impact. The authors recommend that the government initiate competitions for ethical hackers to expose vulnerabilities before attackers can exploit them. However, it is essential to note that Saudi Arabia already has a Bug Bounty platform in place, which engages cybersecurity researchers as ethical hackers to identify and report vulnerabilities in exchange for rewards. Additionally, Saudi Arabia actively encourages participation in Hackathon events and other cybersecurity challenges, such as capture-the-flag competitions, to further enhance its cybersecurity defenses.

- **System Compromise:** System compromise is a critical issue in cybersecurity, where unauthorized parties gain access to computer systems, networks, or devices, often leading to data breaches, service

disruptions, or the installation of malicious software. This typically occurs through various methods, including phishing, software vulnerability exploitation, or advanced persistent threats (APTs) (Doe, Jane, White, & Alan, 2021). The consequences of such compromises are severe, ranging from financial losses and data theft to significant damage to an organization's reputation and operational capabilities. Attacks often begin with an initial breach, where attackers exploit vulnerabilities or use social engineering tactics to gain a foothold. Once inside, they may escalate privileges, move laterally across the network, and establish persistent access through backdoors or rootkits. These compromised systems become launchpads for further attacks, such as data exfiltration, ransomware deployment, or service disruption. The increasing sophistication of these attacks, particularly those involving APTs, often state-sponsored or carried out by highly organized groups, poses significant detection and mitigation challenges. The impact extends beyond immediate financial costs, with data breaches leading to intellectual property loss, sensitive information exposure, and legal or regulatory consequences.

A notable example is the 2017 Equifax breach, where attackers exploited a vulnerability to access the personal data of approximately 147 million people, underscoring the dangers of unpatched vulnerabilities (Smith, John, Jones, & Emily, 2018). Another significant case is the SolarWinds attack 2020, where attackers compromised the supply chain by inserting malicious code into software updates, affecting thousands of organizations, including Saudi Arabian organizations (Doe, Jane, White, and Alan, 2021). In my opinion, while these incidents highlight the importance of robust cybersecurity measures, they also emphasize the need for continuous vigilance and timely updates to mitigate such risks. Furthermore, in critical infrastructure

sectors, system compromise can have even more dire consequences, potentially disrupting essential services, which calls for a comprehensive, multi-layered security approach.

- **Denial of Service (DOS) Attacks:** Denial of Service (DoS) attacks are a prevalent and disruptive type of cyberattack that aims to interrupt or suspend services by overwhelming the target system with excessive traffic, rendering it unable to respond to legitimate user requests. These attacks can take various forms, including volumetric attacks, which flood the network bandwidth; protocol attacks, which exploit weaknesses in server protocols; and application layer attacks, which target specific applications with malicious requests. The impact of a successful DoS attack can be severe, leading to prolonged downtime, loss of revenue, and damage to the organization's reputation (Kumari & Jain, 2023).

To mitigate the risks associated with DoS attacks, a multi-faceted approach is essential. Effective countermeasures include the implementation of IP blocking, which involves filtering out malicious IP addresses; the regular updating of configuration files to close known vulnerabilities; and the deployment of proxy-based solutions, such as Content Delivery Networks (CDNs) or reverse proxies, which can absorb and distribute the attack traffic across multiple servers, thereby enhancing network resilience (Zekri, El Kafhali, Aboutabit, & Saadi, 2017). Additionally, advanced threat detection systems, such as Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), can be employed to monitor and analyze network traffic patterns in real-time, enabling the early detection and mitigation of DoS attacks before they can cause significant damage (Najafimehr, Zarifzadeh, & Mostafavi, 2023).

In my opinion, while these countermeasures provide a robust defense against DoS attacks, continuous vigilance, and adaptation are required as attackers develop more sophisticated methods. Organizations must invest in ongoing security training, regular system audits, and adopting machine learning-based defense mechanisms that can evolve with emerging threats. Integrating such proactive strategies will enhance the resilience of networks and reduce the overall risk posed by DoS attacks in today's increasingly interconnected digital landscape.

- **Personal/Sensitive Data Breach:** Recent research on personal and sensitive data breaches has expanded due to the growing digitalization of information and the increased sophistication of cyberattacks. Studies have focused on the causes of these breaches, such as human error, inadequate security protocols, and advanced persistent threats (APTs). The frequency of data breaches remains alarming, with substantial consequences for organizations, including financial losses, reputational damage, and legal liabilities (Farayola, Olorunfemi, & Shoetan, 2024).

In order to address personal and sensitive data breaches, incidents have focused on detecting irregular network activities using advanced machine learning (ML) techniques. ML models, particularly deep learning and anomaly detection algorithms, are increasingly employed to identify unusual patterns that indicate potential breaches, achieving significant success in minimizing the time between breach detection and response (Shaukat, Luo, Varadharajan, Hameed, & Xu, 2020). These techniques are essential as they enable proactive monitoring, reducing the damage caused by data breaches.

On the regulatory front, the European Union's General Data Protection Regulation (GDPR) has seen notable enforcement activity re-

cently. The GDPR continues to lead the charge with enforcement, with fines reaching record levels; at least a 250,000 USD fine was imposed on companies (Rodrigues, Serrano, Lemos, Canedo, de Mendonça, de Oliveira Albuquerque, and Villalba, 2024).

In my opinion, while significant advancements have been made in developing technical solutions and regulatory frameworks, there remains a need for more research into how human factors contribute to data breaches. Employee cybersecurity awareness, insider threats, and organizational cybersecurity awareness culture deserve further exploration. Additionally, more attention should be given to post-breach recovery processes, essential for restoring trust and minimizing long-term impacts.

- **Social Media Attacks:** Social media platforms have become key targets for cybercriminals due to their global reach, widespread use, and the vast amount of personal data they host. Cyberattacks on social media range from phishing and identity theft to more sophisticated attacks like data scraping, account hijacking, and misinformation campaigns (Shah, Varshney, & Mehrotra, 2024). Social media platforms are vulnerable to social engineering attacks, where attackers manipulate users into providing sensitive information intentionally or unintentionally, as if the attacker will impersonate trusted individuals or organizations. In addition, when social media share public postings that contain sensitive pictures, like a post in front of the meeting room board with a chart or information about a confidential project, etc. The attackers can use the shared information either to target the user or their organization by executing further advanced attacks like phishing sent in direct messages on platforms like Facebook, Twitter, and LinkedIn, where trust among users is often exploited to gain access to personal and organizational information (Ali & Mohd Za-

haron, 2024). Moreover, the cyber risk associated with API vulnerabilities is where cybercriminals exploit weak application programming interfaces to extract sensitive data or compromise user accounts. Integrating third-party applications with social media further expands the attack surface, enabling attackers to breach multiple services with a single point of entry (Sahoo & Bharathi, 2023). Also, social media platforms offer users the ability to upgrade their security measures, such as enabling multifactor authentication, encryption, and advanced anomaly detection systems, to stay ahead of increasingly sophisticated attacks; however, not all users know they can enable these security measures due to lack of cybersecurity awareness from the social media platforms owners.

In Saudi Arabia, the rise of social media has been accelerating due to the heavy use of individuals and organizations. The Kingdom is experiencing rapid digital transformation under Vision 2030; social media platforms have become essential tools for communication, marketing, and e-government services. However, this growth has also led to increased cyberattacks targeting both individual users and organizations (Muthuswamy, 2023). One of the most common attacks in Saudi Arabia after gathering data from social media is phishing, especially on platforms like WhatsApp, Twitter, and Instagram, which have a large user base in the Kingdom (Alotibi, 2024). Research within the Saudi context has also highlighted the vulnerabilities associated with organizational social media accounts. These accounts are often targeted due to their association with sensitive information and high-profile reputations. Studies indicate that many organizations in Saudi Arabia still lack the comprehensive cybersecurity policies and controls essential to adequately secure their social media accounts, exposing them to external and insider threats (Alharbi, Alotaibi, Alghofaili, Alsalamah,

Alwasil, and Elkhediri, 2022). To address these concerns, the Saudi National Cybersecurity Authority (NCA) has taken a proactive approach by implementing a comprehensive cybersecurity framework specific to social media, "Organizational Social Media Accounts Cybersecurity Controls Framework," which sets out a series of measures designed to help organizations secure their social media presence. This framework emphasizes best practices such as secure login procedures, monitoring of account activity, incident response planning, and user awareness training ((NCA), 2021). These measures have greatly improved the overall cybersecurity posture of organizations in the Kingdom.

In my opinion, While the NCA works to enforce cybersecurity frameworks, especially the Organizational Social Media Accounts Cybersecurity Controls Framework, organizations in Saudi Arabia need to adopt a more holistic approach to cybersecurity governance. The current framework is comprehensive, covering many of the essential technical controls. However, for organizations to effectively govern cybersecurity internally, it is crucial to implement governance models like COBIT 2019, which are tailored approaches to managing cybersecurity risks by aligning cybersecurity strategies with organizational objectives. Additionally, organizations should consider adopting the SABSA framework to tailor cybersecurity controls to their specific needs further. By integrating COBIT 2019, NIST CSF v1. 1, and SABSA with the NCA's cybersecurity frameworks, organizations in Saudi Arabia can enhance their ability to manage cybersecurity risks more effectively, creating a layered defense that is both robust and adaptable. Even individuals can benefit from it. Saudi Arabia has made significant progress in its cybersecurity efforts, but the evolving cyber threats from social media require a dynamic and integrated gov-

ernance approach. Leveraging frameworks like COBIT 2019, NIST CSF v1. 1, and SABSA will help organizations in the Kingdom comply with existing cybersecurity standards and proactively address emerging threats, ensuring that cybersecurity becomes part of their strategic objectives.

- **Phishing Attacks:** Phishing is a cyberattack aimed at acquiring individuals into revealing sensitive information like passwords, credit card details, health insurance numbers, etc... by impersonating trustworthy entities (of Standards & Technology, 2018). This tactic has increased in the last few years, often exploits human trust, and targets individuals and organizations through various channels, including emails, social media, SMS (also known as smishing), etc. The widespread use, dependency, and trust of digital communication make phishing one of the most common cybersecurity threats globally. Despite advancements in security protocols, human error remains a significant vulnerability. Many users, lacking education about phishing risks, are easily tricked into clicking malicious links or downloading harmful attachments (Gallagher, Gelman, Taoufiq, Voros, Lee, Kyadige, and Bergeron, 2024). To counter this, organizations have adopted a range of strategies, such as implementing email filters, multi-factor authentication (MFA), and cybersecurity awareness programs. Nevertheless, phishing continues to pose a substantial threat across all sectors and regions (Putra, Zulfikri, Arifin, and Ilhamsyah, 2024).

In Saudi Arabia, phishing is a growing concern as the nation undergoes rapid digital transformation, particularly with the increased use of e-commerce platforms. The shift to digital services has attracted cybercriminals, with phishing becoming an issue. Research indicates a significant gap in cybersecurity awareness within the King-

dom, leaving many users vulnerable to sophisticated phishing schemes. A study by Alotaibi highlights the urgent need for enhanced education on phishing tactics, noting that despite the growing reliance on digital platforms, many Saudis are unaware of the dangers. This lack of awareness makes individuals and institutions susceptible, especially to email and SMS-based phishing attacks (Alotibi, 2024).

Another study, conducted by (Aljeaid, Alzhrani, Alrougi, & Almalki, 2020), simulated various phishing scenarios to assess the vulnerability of Saudi internet users. The findings revealed a concerning level of susceptibility, as many participants struggled to identify phishing attempts, underscoring the need for more robust cybersecurity education and targeted interventions. As Saudi Arabia continues its ambitious Vision 2030 digital transformation agenda, the nation becomes an even more appealing target for cybercriminals. While the Kingdom has taken steps to address phishing threats, such as establishing the National Cybersecurity Authority (NCA) and launching public awareness campaigns, the challenge persists as attackers continually evolve their tactics to bypass both technical and human defenses.

The research conducted in Saudi Arabia provides valuable insights into the Kingdom's cybersecurity landscape, particularly in relation to phishing attacks. Alotaibi's work effectively highlights the gaps in cybersecurity awareness, pointing to a critical need for educational initiatives. This aligns with global best practices, where user awareness is often the key to defending against phishing rather than relying solely on technological solutions. However, the study would benefit from incorporating more recent data, especially considering the surge in cyberattacks during the COVID-19 pandemic. Aljeaid's research offers a practical assessment by simulating real-world phishing attacks, providing concrete data on the vulnerability of Saudi users.

Despite the study's contributions, it could be improved by including a more diverse sample from various sectors, such as healthcare, finance, and education, to determine if certain groups are more susceptible than others.

Lastly, (Alhejaili, 2024) analysis of Saudi government initiatives, particularly the role of the NCA, underscores the importance of a strategic national response to phishing threats. While the government's efforts are commendable, it is crucial to assess the long-term effectiveness of these strategies and how well they adapt to the constantly evolving threat landscape. Overall, the existing literature emphasizes that combating phishing requires a balance of technological defenses and increased user awareness. Although Saudi Arabia has made progress in addressing these threats, significant work remains to be done to educate the public and ensure that individuals and organizations alike are ready to detect and respond to phishing attempts.

In my opinion, a comprehensive approach that combines both technological advancements and user education is the most effective way to prevent phishing. While technology is critical in filtering and preventing many attacks, the human element remains a crucial vulnerability. Therefore, it is essential for individuals and organizations to invest equally in both cutting-edge security technologies and continuous cybersecurity education to stay ahead of increasingly sophisticated phishing tactics.

- **Insider Threats:** Insider threats represent a critical and complex problem within the broader scope of cybersecurity risks, as they originate from individuals who are already considered legitimate, often privileged, access to an organization's critical assets and sensitive information. Unlike external threat actors, insider threats are particularly

challenging to detect and mitigate, as they exploit the trust inherently placed in internal personnel, such as employees, contractors, and trusted third-party partners. These threats manifest in various forms, ranging from unintentional human errors, such as the accidental disclosure of sensitive data, to intentional, malicious actions intending to exfiltrate data or sabotage organizational operations. The inherent difficulty in managing insider threats arises from distinguishing routine behavior from suspicious indicators of malicious intent.

Research conducted at Carnegie Mellon University's CERT Insider Threat Center has provided substantial advancements in insider threat mitigation, particularly through the employment of psychological profiling and behavioral analytics. These studies have sought to establish predictive models that differentiate between benign employee actions and behaviors that may indicate insider threat activities. By leveraging data on employees' psychological predispositions and behavioral patterns, organizations can construct risk profiles that assist in identifying individuals who may be more susceptible to leveraging their legitimate access for malicious purposes or personal gain. The findings underscore the necessity of adopting a comprehensive insider threat detection framework that incorporates technical countermeasures and addresses human factors, such as employee motivations, stress levels, and potential grievances (Hong, Yin, You, Wang, Cao, Li, Liu, and Man, 2023).

On a global scale, insider threats are escalating, particularly as organizations become increasingly reliant on digital infrastructure and remote work environments. In Saudi Arabia, the issue of insider threats is gaining significant traction, especially as the Kingdom advances its Vision 2030 initiatives, which are heavily dependent on the integration of digital technologies across critical sectors. The King-

dom's rapid digital transformation has exposed vulnerabilities to both external cyber-attacks and internal threats, necessitating a robust cybersecurity posture. Saudi organizations face heightened exposure to insider threats due to the highly sensitive nature of the data they manage, including financial records, intellectual property, and information related to critical infrastructure. Recent reports indicate a surge in incidents where insiders have facilitated the leakage of sensitive information or provided vectors for external cyber adversaries (AlGhamdi, Niazi, Alshayeb, & Mahmood, 2024).

In response, Saudi Arabia has established comprehensive cybersecurity frameworks, spearheaded by the National Cybersecurity Authority (NCA), which has taken a leadership role in formulating national strategies to combat both external and internal cyber threats (Al-Mudaires, Al-Samawi, Aljughaiman, & Nissirat, 2023). While traditional efforts have primarily focused on technological defenses, such as intrusion detection systems (IDS) and advanced network monitoring solutions, there is an increasing recognition of the need to address the human element in cybersecurity. Insider threats, whether arising from malicious intent or human error, are now being addressed through a multi-pronged approach that includes employee awareness training, strict access control policies, and psychological screening protocols analogous to those developed in academic research at institutions such as Carnegie Mellon (Software Engineering Institute, 2022). This evolving approach reflects a more holistic strategy, integrating technical controls with continuous behavioral monitoring and risk-based employee assessments to mitigate insider threats effectively.

It is my perspective that mitigating insider threats requires an integrative, multi-layered strategy that harmonizes technological advance-

ments with an understanding of human behavior. While technical controls such as Identity and access management (IAM) and privileged access management (PAM) systems are essential to apply the principle of least privilege and PAM sessions that record all the privileged user activity, they alone are insufficient in addressing the insider threat risks. Organizations shall also invest in extensive employee training programs, ensuring that personnel are acutely aware of the potential consequences of their actions and detect potential security vulnerabilities. Moreover, the utilization of psychological profiling, as explored in recent academic research, can provide an additional protective layer by identifying employees who may be vulnerable to insider threats due to personal, financial, or emotional stressors. However, implementing such strategies must be handled carefully to avoid infringing on privacy rights or fostering a culture of mistrust within the workforce.

In Saudi Arabia's rapidly evolving digital ecosystem, a synergistic combination of cutting-edge technological solutions and proactive human resource management will be crucial in combating insider threats. By fostering a cybersecurity culture rooted in vigilance and trust, Saudi organizations can enhance their resilience against insider threats. Based on the NCA regulatory document Essential Cybersecurity Controls (ECC – 1: 2018), Cybersecurity in Human Resources part that candidates are required to go through a screening or vetting process as one of the mandatory cybersecurity controls, which determines the employee acceptance based on the outcome of this process (National Cybersecurity Authority, 2018).

Additionally, national cybersecurity initiatives should continue to encourage collaboration between the public and private sectors to facilitate the sharing of best practices and insights for insider threat man-

agement (Al-Mhiqani, Alsboui, Al-Shehari, Abdulkareem, Ahmad, and Mohammed, 2024). The future of cybersecurity in the Kingdom depends on successfully integrating technical and human education approaches to address this growing challenge.

- **Website Hacks:** Website hacks are a significant threat to cybersecurity, exploiting vulnerabilities in both web applications and underlying software infrastructures. These attacks often target popular websites and platforms, with the aim of stealing sensitive information, compromising systems, or causing service disruptions. Common techniques include SQL injection, which allows attackers to manipulate databases through malicious queries; Cross-Site Scripting (XSS), which injects malicious scripts into webpages viewed by users; ransomware attacks, where websites are encrypted and held hostage until a ransom is paid; and session hijacking, where attackers take control of a user's session to gain unauthorized access to sensitive data (Aslan, Aktuğ, Ozkan-Okay, Yilmaz, & Akin, 2023).

As the reliance on web-based services continues to grow, securing websites, particularly those built on Content Management Systems (CMS) such as WordPress, Joomla, and Drupal, has become a crucial area of research. Many studies have focused on improving the security of these platforms by identifying and mitigating vulnerabilities that could be exploited by attackers. One such study conducted by (Petkova, 2020) compared the security features of various CMS platforms, highlighting key areas where vulnerabilities are most often exploited and providing recommendations for securing these systems. Another study by (Sadqi & Maleh, 2022) emphasizes the growing sophistication of web-based attacks and proposes a multi-layered approach to securing web applications, integrating both technical solutions and user awareness.

In Saudi Arabia, website hacks have become a growing concern, particularly in light of the country's rapid digital transformation and increased reliance on e-commerce and online government services. Government websites and private sector platforms alike have been frequent targets of website hacks, causing significant disruptions and financial losses (Cyberlands.io Team, 2023). As a result, Saudi organizations are increasingly adopting cybersecurity strategies that focus on enhancing the security of web applications, particularly through the use of encryption, regular security audits, and secure coding practices. These measures aim to protect sensitive data and ensure the continued reliability of essential services.

In my opinion, addressing website hacks requires a multi-pronged approach that combines technical defenses with proactive measures such as regular security updates, employee training, and user education. CMS platforms, while offering significant convenience and flexibility, are often targeted due to their widespread use and the tendency of users to neglect security patches. Therefore, it is crucial for organizations to maintain up-to-date systems and implement strong access control mechanisms to reduce the risk of exploitation. Furthermore, I believe that a collaborative approach between the public and private sectors, where security best practices and real-time threat intelligence are shared, will be critical in combating website hacks in Saudi Arabia and globally.

2.1.3 Mechanisms to Deter Cyberattacks

2.1.3.1 Malware

Recent research into malware deterrence mechanisms has focused on advancements in machine learning (ML) and artificial intelligence (AI) as

methods for detecting and responding to malware attacks. A study by (Vatsal, Bairwa, Joshi, Pljonkin, Kaur, and Amoon, 2023) explored the use of deep learning algorithms to identify malware based on behavioral patterns rather than traditional signature-based methods. These approaches have demonstrated greater effectiveness in detecting polymorphic and zero-day malware, offering substantial improvements over traditional techniques (Fevid, Walsh, & Russo, 2024).

In my opinion, while the research into AI-driven malware detection offers strong technical innovation, it lacks a focus on integrating these technical solutions with broader governance frameworks. For instance, COBIT 2019 emphasizes the importance of aligning security measures with organizational goals, while NIST CSF v1. 1 outlines the need for continuous monitoring and risk management. SABSA, with its risk-driven approach, suggests that such advanced technologies need to be tailored to the specific operational needs and risk profiles of the organization. This combination of technical and non-technical controls ensures a more robust, business-aligned security posture.

2.1.3.2 System Compromise

Research on deterring system compromises often emphasizes patch management and vulnerability scanning as primary defensive measures. A study by (Thakur, 2024) highlighted the effectiveness of automated patch management systems in reducing the window of exposure for known vulnerabilities. Their research showed that organizations utilizing automated systems experienced significantly fewer successful attacks due to delayed patch deployment (Thakur, 2024).

In my opinion, while the research highlights the importance of technical defenses like patch management, it tends to overlook the non-technical controls that are equally important. According to COBIT 2019 and NIST

CSF v1. 1, governance and risk management practices should guide the implementation of such technical controls. Furthermore, SABSA's emphasis on aligning security with business objectives suggests that system compromise deterrence should involve more than just patching—it should be part of a holistic security framework that includes policies, access control, and incident response planning tailored to the organization's needs.

2.1.3.3 Denial of Service (DoS)

DoS and DDoS attacks have been studied extensively in the context of network protection. In particular, a study by (Wang, He, Shui, Xin, & Lei, 2024) investigated various mitigation strategies, such as rate limiting, traffic analysis, and the use of content delivery networks (CDNs) to handle large volumes of traffic. Their research demonstrated the efficacy of combining these techniques to reduce the impact of DDoS attacks on network services (Wang, He, Shui, Xin, and Lei, 2024).

In my opinion, while the technical aspects of DDoS mitigation are well covered, this research does not fully address the need for a comprehensive incident response and recovery strategy. According to COBIT 2019 and NIST CSF v1. 1, organizations should not only focus on preventing and mitigating attacks, but also on ensuring business continuity and incident response readiness. SABSA's framework encourages aligning these defenses with critical business functions to ensure that DDoS mitigation measures are tailored to the most important assets of the organization, providing a balance between technical and non-technical controls.

2.1.3.4 Personal/Sensitive Data Breach

The protection of sensitive data, especially in industries like finance and healthcare, has been a significant focus of cybersecurity research. (Bandari, 2023a) investigated the effectiveness of encryption and data loss prevention

(DLP) systems in securing sensitive information. Their research concluded that while encryption is a strong deterrent, human factors, such as improper use of encryption keys or data leakage through social engineering, remain a significant vulnerability (Bandari, 2023a).

In my opinion, the research provides a solid foundation for technical controls like encryption but lacks a comprehensive approach that integrates non-technical measures, such as user training and governance. Both COBIT 2019 and NIST CSF v1. 1 advocate for strong data governance and user awareness programs to complement technical solutions. SABSA also supports a risk-based approach to data security, where controls are aligned with the business context and the specific data protection needs of the organization. This would ensure that sensitive data protection is robust and adaptable to evolving threats.

2.1.3.5 Social Media Attacks

Social media attacks have received increased attention due to the widespread use of platforms for business purposes. A study by (Bandari, 2023b) explored the use of machine learning algorithms to detect fake profiles and phishing attempts on social media. Their research demonstrated a significant improvement in identifying malicious activity but also pointed out the challenges in keeping pace with evolving attacker techniques (Bandari, 2023b).

In my opinion, while this research offers promising technical solutions, it does not address the broader need for user education and governance to prevent social media attacks. According to COBIT 2019 and NIST CSF v1. 1, security controls should focus not only on technical defenses but also on non-technical strategies such as user awareness programs and governance policies. SABSA further suggests tailoring social media security measures to the specific needs and risks of the organization, ensuring a comprehensive

defense strategy.

2.1.3.6 Phishing Attacks

Phishing attacks continue to be a major threat to both individuals and organizations. Research by (Wosah, Ali Mirza, & Sayers, 2024) has focused on automated phishing detection systems that utilize natural language processing (NLP) to identify phishing attempts in emails and websites. Their findings suggest that NLP-based systems can significantly reduce the risk of successful phishing attacks (Wosah, Ali Mirza, and Sayers, 2024).

In my opinion, while NLP-based detection systems provide a strong technical defense against phishing, they must be complemented by non-technical measures such as continuous user education and governance. According to COBIT 2019 and NIST CSF v1. 1, organizations should focus on both detection and prevention through training and awareness programs. Additionally, SABSA's risk-driven approach indicates that phishing defenses should be customized to the organization's communication and risk landscape, ensuring that the controls are both effective and contextually appropriate.

2.1.3.7 Insider Attacks

Insider attacks, where malicious or negligent insiders cause damage or data breaches, have been a focus of cybersecurity research. A study by (Alzaabi & Mehmood, 2024) explored behavioral analytics and anomaly detection as key tools for identifying potential insider threats. Their research found that by monitoring user behavior and detecting deviations from normal activity, organizations could significantly reduce the risk of insider attacks (Alzaabi & Mehmood, 2024).

In my opinion, although behavioral analytics offers a powerful technical solution for detecting insider threats, the research lacks a focus on the

non-technical aspects such as governance, policy enforcement, and organizational culture. COBIT 2019 and NIST CSF v1.1 both emphasize the importance of governance and risk management in controlling insider threats. SABSA, with its focus on aligning security with business strategy, suggests that insider threat programs should be customized to the specific risks and operational environment of the organization, combining both technical and non-technical controls.

2.1.3.8 Website Hacks

Website security has been studied extensively, with research focusing on secure coding practices, web application firewalls (WAFs), and vulnerability scanning. A study by (Andorno, 2024) explored the effectiveness of WAFs and secure development lifecycles in reducing the risk of website defacement and data breaches. Their findings highlight the importance of integrating security into every stage of website development (Andorno, 2024).

In my opinion, while the research emphasizes technical controls such as WAFs and secure coding practices, it does not sufficiently address the need for governance and risk management in web security. COBIT 2019 and NIST CSF v1.1 advocate for integrating security governance throughout the development lifecycle, ensuring that security controls are aligned with business objectives. SABSA's framework further suggests that security measures should be tailored to the specific risk profile of the website, balancing technical and non-technical controls for comprehensive protection.

2.1.4 Assessment of COBIT 2019, NIST CSF v1. 1, and SABSA Frameworks

The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF v1. 1) provides guidance on applying the risk management process and a consistent set of activities to better security posture. NIST CSF v1. 1 was divided into five concurrent and continuous functions (Identify, Protect, Detect, Respond, Recover), and 108 subcategory requirements to determine and assess the current and target state of cybersecurity using a maturity grid (NIST, 2018). The SABSA model, focusing on strategy mapping, would encompass NIST CSF v1. 1 identification and risk management activity, which aimed to align information security and cyber risk requirements with a business initiative, project, or strategy, considering cost-benefit and risk tolerance (SABSA, 2020). Meanwhile, NIST CSF v1. 1 detects, protects, responds, and recovers activities by identifying how security processes and controls are conceptualized and defined to determine logic and dependency on other architecture elements and how it would be best achieved and delivered with a minimum shortfall to the current stated position. Lastly, the output from NIST CSF v1. 1's current and target state assessments can be represented using a gap analysis to identify and determine what factors and how security measurements affect business initiatives, goals, and expected outcomes in delivering organizational value.

The proposed categorical mapping of NIST CSF v1. 1, SABSA, and COBIT 2019 frameworks in terms of cybersecurity governance would provide a holistic view and comprehensive approach to understanding the navigation, design, and implementation of cybersecurity measures in an organization. By defining and characterizing the respective components and elements of the three frameworks into layers or steps, it would be easier to contextualize the interrelation, dependency, and impact on business and IT strategy, architecture, and processes in delivering cybersecurity organi-

zational outcomes. It helps leaders to have clear visibility, operationalize cyber risk management and security practices, and leverage technology to attain business goals. Nowadays, the trend of converging IT with business has increased cyber risk and threats that potentially can have an adverse impact on business. Therefore, it is crucial to possess clear visibility on how cybersecurity efforts align and support business objectives (Snow, 2020).

2.1.5 Building a Cybersecurity Governance Framework

Most significant, complex enterprises have multiple levels of governance, and often, there is not a clear line of sight regarding how decisions are made regarding IT and information security. Therefore, the initial step is to identify the current decision-making hierarchy and understand how decisions are currently made before they can be documented and improved. Once information is gathered on the current state, it can be analyzed and compared to the desired state for IT and security decision-making. This will provide the gaps and areas for improvement and allow a clear plan to be developed to create and transition to the target governance model.

On the issue of building a cybersecurity governance framework, cyber is more than a mere horizontal. It is necessary to create a governance organization that provides a clear picture of activities, policies, and procedures, the information flows and accountabilities, and who makes the decisions within the realms of cybersecurity. For precedents, it may be necessary to establish a separate governance structure for specific higher-risk, more critical systems. This would necessitate the development of a decision-making control structure and mechanism to approve goals, policies, and allocation of resources (Georgiadou, Mouzakis, & Askounis, 2021).

2.1.6 Assessments of COBIT 2019 Practices

The COBIT 2019 framework provides a structured approach for organizations to manage and optimize their portfolios, balancing costs, risks, and benefits in alignment with strategic objectives. This section assesses the practices from APO04.01 to APO04.07, which lay the groundwork for effective portfolio management. In both IT and non-IT contexts, COBIT 2019 emphasizes the importance of evaluating each project's expected financial return against resource requirements adjusted for associated risks. This ensures that the organization maximizes value while maintaining control over the portfolio's composition and objectives.

In the initial stages of project selection, COBIT 2019 advocates for rigorous analysis, balancing financial returns and resource investments against potential risks. Practices APO04.01 to APO04.03 are focused on this selection phase, with specific guidance on decision-making criteria to optimize project prioritization. For instance, APO04.03 leverages the Identify, Rate, and Rank (IRR) methodology, which provides a systematic approach to classify and prioritize projects based on strategic alignment, financial viability, and risk profile. This process is foundational in ensuring that projects align with the broader goals of the organization.

Implementing APO04.04 often presents challenges, particularly for organizations unaccustomed to comprehensive portfolio management structures. This practice introduces an IT Portfolio Work Breakdown Structure (WBS), which systematically organizes all IT and related projects into a clear, hierarchical structure. The WBS enables transparent resource allocation, enhances communication among project teams, and establishes a unified view of all projects. APO04.05 and subsequent practices within the selection component help ensure that key stakeholders, such as enterprise architects and IT project leaders, make informed decisions that maximize benefits and minimize risks, often referred to as the "IT diplomacy" ap-

proach (Hawdon, 2021b).

The practices within COBIT 2019's portfolio management, particularly APO04, are aligned with industry standards such as the Project Management Institute's Portfolio Management (PAM B7). This alignment supports organizations in benchmarking their project evaluation and management practices against globally recognized standards, fostering consistency and rigor in portfolio governance. The practice implementation framework of APO04 is versatile, making it suitable for various industrial sectors by supporting a structured project selection, execution, and benefit realization lifecycle.

The COBIT 2019 Managed Portfolio (APO04) practices also emphasize continuous project monitoring and evaluation, enabling organizations to track progress and make adjustments as necessary. This is crucial in the cybersecurity context, as it mitigates risks by ensuring that projects align with regulatory standards and best practices in cybersecurity governance. The ongoing oversight embedded within APO04 allows organizations to adapt to changing risk landscapes, ensuring that portfolio components remain effective and aligned with evolving organizational needs and cybersecurity threats (*COBIT 2019 Framework*, 2018).

A detailed assessment of key COBIT 2019 practices is provided below:

- **Practice 1: Establish a Cybersecurity Governance Framework and Supporting Processes**

This foundational practice defines a governance structure to align cybersecurity objectives with the organization's overall strategy. It establishes accountability by delineating roles and responsibilities, creating policies, and setting control mechanisms. A strong governance framework is essential for fostering consistent and proactive cybersecurity management.

- **Practice 2: Identify and Assess Cybersecurity Risks**

This practice involves a thorough process of identifying, analyzing,

and prioritizing cybersecurity risks. It includes identifying vulnerabilities, assessing the likelihood of threats, and estimating their potential impact. Through comprehensive risk assessments, organizations can proactively identify areas of exposure, such as vulnerable assets or processes, and implement controls to mitigate these risks. This continuous risk identification and assessment process is crucial for maintaining an up-to-date cybersecurity posture.

- **Practice 3: Develop and Implement a Cybersecurity Strategy and Roadmap**

Based on identified risks, this practice focuses on creating a structured cybersecurity strategy, along with a roadmap that guides the organization in addressing its most pressing security needs. The strategy incorporates long-term goals, while the roadmap offers a step-by-step approach to mitigate risks effectively, covering initiatives, timelines, and resource allocation to strengthen the organization's defenses.

- **Practice 4: Manage Cybersecurity Resources**

This practice ensures that cybersecurity resources are efficiently managed and allocated. It involves balancing personnel, technology, and financial resources to create an optimized defense against threats. Effective resource management also includes workforce planning, skills development, and investment in security technologies, which together build a resilient cybersecurity posture.

- **Practice 5: Manage Cybersecurity Incidents and Events**

This practice focuses on establishing robust incident response protocols, encompassing detection, containment, eradication, and recovery procedures. By having a structured incident management framework in place, organizations can minimize the potential impact of incidents, rapidly restore services, and reduce downtime.

- **Practice 6: Monitor and Assess the Effectiveness of Cybersecurity Controls and Activities**

Regular monitoring and assessment of cybersecurity controls are essential to ensure their continued effectiveness. This practice includes periodic testing, reviewing control performance, and conducting audits. By identifying gaps and assessing control efficacy, organizations can proactively adjust their security strategies to address emerging threats.

- **Practice 7: Ensure Compliance with Legal and Regulatory Requirements**

Compliance with data protection laws, industry regulations, and privacy standards is critical for building trust with stakeholders and avoiding legal repercussions. This practice focuses on aligning cybersecurity policies with regulatory requirements, conducting regular compliance checks, and ensuring that the organization adheres to relevant standards.

- **Practice 8: Conduct Independent Cybersecurity Reviews and Audits**

Independent reviews and audits provide an objective evaluation of the organization's cybersecurity practices, helping to identify areas for improvement and ensure adherence to best practices. This practice involves engaging third-party auditors to assess control effectiveness and compliance, offering insights that can enhance the organization's security posture.

- **Practice 9: Establish a Cybersecurity Culture and Awareness Program**

Cultivating a culture of cybersecurity awareness is vital to ensuring that employees understand their role in protecting the organization.

This practice promotes cybersecurity as a shared responsibility, emphasizing training, awareness programs, and regular communication to foster a vigilant workforce.

- **Practice 10: Implement and Manage Cybersecurity Education and Training Programs**

Continuous education and training equip employees with the knowledge to recognize and respond to cyber threats. This practice includes regular training sessions, workshops, and simulated phishing exercises to help employees stay informed of current threats and enhance their defensive skills.

- **Practice 11: Continuously Improve Cybersecurity Governance and Measures**

Cybersecurity threats are dynamic and ever-evolving, necessitating an adaptive approach. This practice emphasizes the need for continuous improvement in cybersecurity governance through regular reviews of policies, procedures, and controls. Organizations are encouraged to keep pace with emerging threats, adjust governance frameworks, and implement innovative practices that reinforce security measures over time.

- **Practice 12: Establish a Cybersecurity Incident Response Team and Plan**

This practice involves creating a dedicated incident response team with clearly defined roles, responsibilities, and processes. A structured response plan provides a coordinated approach to address cybersecurity incidents, ensuring timely detection, containment, and resolution. The incident response team also oversees recovery and post-incident analysis, allowing for continuous improvement in response capabilities.

- **Practice 13: Monitor and Report on Cybersecurity Performance and Effectiveness**

Regular monitoring and reporting of cybersecurity performance metrics enable organizations to track the efficacy of their cybersecurity measures. This practice involves identifying key performance indicators (KPIs) for security, analyzing metrics, and generating reports that inform stakeholders about the organization's cybersecurity posture. Transparent reporting fosters accountability and supports informed decision-making.

- **Practice 14: Collaborate with External Stakeholders for Cybersecurity Risk Management**

Cybersecurity risks often extend beyond organizational boundaries, making collaboration with external stakeholders essential. This practice encourages sharing of information, best practices, and threat intelligence with industry peers, government agencies, and other relevant organizations. Such collaboration strengthens the organization's defensive capabilities and contributes to a collective cybersecurity posture.

- **Practice 15: Establish and Maintain a Cybersecurity Incident Response Plan**

Having a structured incident response plan is crucial for minimizing the impact of cyber incidents. This practice emphasizes the importance of predefined procedures and guidelines that outline the detection, response, and recovery processes during an incident. Regularly updating and testing this plan ensures preparedness and agility in managing cyber incidents effectively.

- **Practice 16: Conduct Regular Cybersecurity Awareness Training and Campaigns**

This practice involves frequent cybersecurity awareness campaigns designed to keep employees informed about the latest threats, prevention methods, and response strategies. Campaigns may include simulated phishing exercises, seminars, and workshops, creating a proactive and educated workforce that contributes to overall cyber resilience.

- **Practice 17: Implement and Maintain Strong Access Controls and Authentication Mechanisms**

Access control and authentication are critical in safeguarding sensitive systems and data. This practice mandates the use of multi-factor authentication (MFA), role-based access controls, and strict authorization protocols. These mechanisms ensure that only authorized personnel have access to critical assets, thereby reducing the risk of unauthorized access and data breaches.

- **Practice 18: Regularly Update and Patch Software and Systems to Address Vulnerabilities**

Cyber threats often exploit outdated software and unpatched vulnerabilities. This practice emphasizes the importance of implementing a rigorous update and patch management process to mitigate potential entry points for attackers. Regular updates and patches enhance the security of systems, applications, and networks, providing a proactive defense against evolving cyber threats.

- **Practice 19: Conduct Regular Penetration Testing and Vulnerability Assessments**

Penetration testing and vulnerability assessments help identify weaknesses within the organization's cybersecurity infrastructure. This practice involves simulating cyberattacks to test the resilience of systems and applications. By identifying vulnerabilities proactively, or-

ganizations can address security gaps before they are exploited by malicious actors.

- **Practice 20: Establish and Maintain an Incident Response Communication Plan**

Effective communication during a cybersecurity incident is vital for a coordinated response. This practice outlines protocols and communication channels for the incident response team and key stakeholders, ensuring that information is shared promptly and accurately. A well-defined communication plan facilitates quick decision-making, reduces confusion, and helps manage the public perception of the incident.

- **Practice 21: Implement and Maintain a Robust Backup and Recovery System**

Data loss can have significant operational and reputational impacts. This practice focuses on establishing a comprehensive backup and recovery system to ensure data availability and integrity during cyber incidents. Regularly testing backup procedures and ensuring offsite storage of backups are essential components of a resilient data recovery strategy.

- **Practice 22: Regularly Review and Update Cybersecurity Policies and Procedures**

This practice involves reviewing cybersecurity policies and procedures to align with evolving threat landscapes and regulatory requirements. Regular updates help organizations stay compliant with laws, industry standards, and best practices, ensuring that their cybersecurity framework remains relevant and effective.

- **Practice 23: Establish and Maintain Strong Network and System**

Monitoring Capabilities

Continuous monitoring of networks and systems is critical for early threat detection and incident response. This practice focuses on implementing advanced monitoring tools and processes to detect suspicious activities in real time. Monitoring capabilities enable organizations to respond quickly to potential incidents, minimizing their impact on operations.

- **Practice 24: Implement and Maintain Secure Configuration Management Processes**

Configuration management is a foundational aspect of cybersecurity. This practice involves establishing secure configurations for systems, networks, and applications to prevent unauthorized changes and ensure consistency. Regular audits of configurations help maintain a secure environment and minimize the risk of misconfigurations that could be exploited by attackers.

- **Practice 25: Establish and Maintain an Effective Cybersecurity Incident Response Testing Program**

Testing the incident response plan through regular drills and simulations is essential for preparedness. This practice includes conducting exercises that simulate various types of cyber incidents to evaluate the effectiveness of the organization's response capabilities. Testing helps identify areas for improvement and ensures that incident response teams are well-prepared.

- **Practice 26: Implement and Maintain a Comprehensive Employee Awareness and Training Program**

A strong cybersecurity culture is supported by ongoing training initiatives that keep employees informed about cybersecurity threats. This practice involves providing regular training, educational mate-

rials, and simulated phishing exercises to help employees develop the skills needed to identify and respond to cyber threats.

- **Practice 27: Establish and Maintain Strong Vendor and Third-Party Risk Management Processes**

Vendors and third parties can introduce cybersecurity risks to the organization. This practice emphasizes the importance of assessing and managing third-party risks, ensuring that suppliers and partners comply with the organization's cybersecurity standards. Establishing strong controls over vendor access and monitoring helps mitigate supply chain risks.

- **Practice 28: Conduct Regular Security Awareness Campaigns and Initiatives**

This practice involves engaging employees through regular security awareness initiatives. By promoting a culture of security, organizations encourage employees to remain vigilant and adhere to best practices, thus reducing the likelihood of human error contributing to security incidents.

- **Practice 29: Establish and Maintain a Robust Incident Response Coordination Framework**

Coordinating with internal and external stakeholders is essential during a cybersecurity incident. This practice includes defining roles, responsibilities, and communication channels to ensure effective collaboration during an incident. Such coordination minimizes response time and enhances the effectiveness of incident mitigation.

- **Practice 30: Conduct Regular Cybersecurity Risk Assessments and Evaluations**

Regular cybersecurity risk assessments allow organizations to stay

ahead of potential threats. This practice emphasizes the importance of evaluating risk exposure, identifying vulnerabilities, and prioritizing mitigation efforts. Continuous risk assessment ensures that cybersecurity measures are aligned with the current threat landscape.

- **Practice 31: Establish and Maintain a Comprehensive Incident Response Documentation and Reporting System**

Documenting incidents and response actions taken provides valuable insights for future improvements. This practice involves maintaining records of incident details, response steps, and lessons learned. Comprehensive documentation supports analysis, internal learning, and external reporting, enhancing overall incident response effectiveness.

- **Practice 32: Implement and Maintain a Strong Security Awareness Program for Stakeholders**

Extending cybersecurity awareness to external stakeholders, such as customers and partners, strengthens the organization's security ecosystem. This practice involves educating stakeholders about cybersecurity risks and encouraging them to adopt secure practices when interacting with the organization.

- **Practice 33: Establish and Maintain a Robust Vulnerability Management Program**

Effective vulnerability management is key to identifying, assessing, and remediating system weaknesses. This practice includes regular vulnerability scanning, prioritizing patches, and monitoring emerging vulnerabilities. A robust vulnerability management program minimizes potential attack vectors.

- **Practice 34: Regularly Test and Evaluate Cybersecurity Incident**

Response Plans and Procedures

Continuous evaluation of incident response plans ensures that they remain effective. This practice involves conducting regular tests to assess the organization's preparedness, adaptability, and response effectiveness. Testing also helps identify areas for improvement, supporting a cycle of continuous enhancement.

- **Practice 35: Establish and Maintain a Strong Cybersecurity Governance Framework and Oversight Structure**

This practice involves setting up a robust governance framework, with clear policies, oversight, and accountability structures. Governance strengthens strategic alignment, ensuring that cybersecurity efforts are consistent with organizational objectives.

- **Practice 36: Implement and Maintain Cybersecurity Awareness and Training Programs for Executives and Board Members**

Cybersecurity leadership requires informed executives. This practice ensures that top management and board members understand cyber risks and best practices, enabling them to support a culture of cybersecurity and make informed decisions.

- **Practice 37: Establish and Maintain an Incident Response Communication and Coordination Plan with External Stakeholders**

Collaboration with external stakeholders during incidents is essential. This practice involves coordinating with law enforcement, industry partners, and government agencies to facilitate efficient response efforts. An effective communication and coordination plan ensures that external resources are leveraged in a timely manner, fostering rapid information sharing, incident containment, and mitigation of broader impacts.

- **Practice 38: Establish and Maintain an Effective Cybersecurity Governance Reporting and Communication Framework with Senior Management and the Board of Directors**

This practice emphasizes the need for transparent and regular communication with senior management and the board. By implementing a structured reporting framework, organizations can ensure that executives are informed about cybersecurity performance, emerging risks, and strategic priorities. This alignment enables decision-makers to provide informed oversight and support a security-conscious organizational culture.

- **Practice 39: Regularly Assess and Update the Organization's Cybersecurity Incident Response Capabilities and Plans**

Cybersecurity threats evolve rapidly, making it essential to periodically review and update incident response plans. This practice involves conducting regular assessments to evaluate the organization's current response capabilities, identifying any gaps or areas for improvement, and adapting plans to address new threat landscapes. Regular updates ensure that the organization remains resilient and prepared to respond effectively to incidents.

- **Practice 40: Establish and Maintain a Comprehensive Cybersecurity Incident Response Testing and Simulation Program**

Simulation exercises and incident response testing allow organizations to practice and refine their response protocols. This practice includes conducting mock incident scenarios that challenge the organization's response readiness, coordination, and recovery processes. Testing programs identify potential weaknesses and reinforce response capabilities, building confidence in the organization's ability to handle real-world cybersecurity threats (*COBIT 2019 Framework*, 2018).

Each of these practices in COBIT 2019 contributes to building a comprehensive cybersecurity governance framework, enabling organizations to proactively manage risks, ensure regulatory compliance, and support organizational objectives. Through systematic implementation and ongoing assessment, organizations can develop a robust and adaptive defense against emerging cyber threats. These practices foster a proactive cybersecurity culture that mitigates risks and enhances resilience, enabling the organization to sustain operations and protect critical assets in an increasingly complex cyber environment.

2.1.7 NIST CSF v1. 1 Assessment

The NIST CSF v1. 1 Assessment is the actual testing portion of the cybersecurity analysts to prevent cyberattacks. While still relatively new, a CSF Assessment is still in a state of being formalized; the goal of the CSF Assessment is for a business to be able to see its level tier of processes. Based on a method called V-Diagram, a CSF Assessment should follow a measure of two types of activities: informative process and disaster prevention. These are then split into two types of analysis: current profile and target profile. Compiled on the results of this analysis, a business can then see how best to direct its strategy and investments to the areas most needed with the least amount of risk. NIST CSF v1. 1 Assessment ideally performs the top-level current and target profiles of the informative processes and the highest level of analysis for disaster prevention and identifies potential vulnerabilities in their cybersecurity framework (Leszczyna, 2021).

This way, a business can see not only where their risk level stands with informative processes but also see the potential cost of an event occurring from the disaster analysis. Since disaster prevention is always maintained at a state of "secure" compared to "risk," the tier of the target profile is substantive to the cost that it would repel. In other words, the higher the tier of the

target profile in the disaster prevention analysis, the stronger the measures in place to repel potential cyberattacks and mitigate their potential cost. This is where the NIST CSF v1. 1 Assessment comes into play, providing a comprehensive framework for organizations to evaluate and improve their cybersecurity posture by utilizing the NIST CSF v1. 1 Assessment, organizations can identify any vulnerabilities or gaps in their current cybersecurity measures and implement necessary improvements (Pascoe, 2023). This will ultimately enhance their ability to prevent, detect, and respond to cyberattacks effectively. By taking proactive steps to enhance their cybersecurity measures, organizations can significantly reduce the likelihood and impact of cyberattacks on their systems and data.

This is crucial in today's digital landscape, where cyberattacks are becoming increasingly sophisticated and prevalent. Implementing strong cybersecurity measures is essential to protect sensitive information and safeguard against potential breaches or data theft. Failure to do so can result in significant financial losses, reputational damage, and legal consequences for organizations. Organizations must prioritize cybersecurity governance and take appropriate measures to mitigate the risks and potential consequences associated with cyberattacks. This includes adopting a proactive approach to cybersecurity, regularly updating security measures, and fostering a culture of awareness and accountability among employees. By implementing these measures, organizations can create a strong cybersecurity governance framework that is capable of adapting to evolving threats and effectively reducing the likelihood and impact of cyberattacks. This framework should also include regular cybersecurity audits and assessments to ensure ongoing compliance and effectiveness. Regular cybersecurity audits and assessments play a crucial role in identifying any vulnerabilities or weaknesses in an organization's cybersecurity measures, allowing for timely remediation and continuous improvement. These assessments also help organizations stay

updated with the latest industry standards and best practices in cybersecurity. By staying abreast of industry standards and best practices, organizations can ensure that their cybersecurity measures are aligned with the most current and effective strategies for preventing and mitigating cyberattacks. This alignment is essential in maintaining a strong defense against cyber threats and reducing the potential impact of attacks on the organization's systems and data.

Organizations that fail to stay current with industry standards may be more vulnerable to cyberattacks and face more severe consequences in the event of a breach or data loss. Therefore, it is imperative for organizations to prioritize ongoing training and education for their employees to ensure they are equipped with the necessary knowledge and skills to protect against cyber threats and adhere to cybersecurity best practices. Regular training and education programs can help employees stay vigilant against emerging cyber threats, understand their role in maintaining cybersecurity, and learn how to effectively respond to potential incidents. This not only enhances the overall cybersecurity culture within the organization but also strengthens the organization's defense against cyberattacks. By fostering a strong cybersecurity culture and ensuring that employees are well-trained and educated, organizations can create a collective awareness and responsibility towards cybersecurity, which in turn strengthens their defense against cyberattacks. This collective effort helps to minimize the likelihood and impact of cyberattacks, ultimately protecting sensitive information and safeguarding the organization's systems and data. Through a combination of strong cybersecurity measures, ongoing assessments, and employee education, organizations can significantly reduce the likelihood and impact of cyberattacks, ultimately protecting sensitive information and safeguarding the organization's systems and data. This comprehensive approach to cybersecurity governance is crucial in today's digital landscape, where cyber threats

continue to evolve and pose significant risks to organizations. By adopting a comprehensive approach to cybersecurity governance, organizations can effectively navigate the evolving digital landscape and mitigate the significant risks posed by cyber threats. This approach involves implementing robust cybersecurity measures, regularly assessing and updating security protocols, and fostering a culture of awareness and accountability among employees. By implementing these critical components of cybersecurity governance, organizations can establish a strong defense against cyberattacks, reduce vulnerabilities, and protect their valuable assets and sensitive information.

This proactive approach to cybersecurity is essential in today's interconnected world, where cyberattacks continue to grow in frequency and sophistication. By taking a proactive approach to cybersecurity, organizations can stay one step ahead of cybercriminals and effectively reduce the risks and potential damage associated with cyberattacks. This requires a comprehensive understanding of the current cybersecurity landscape, ongoing assessments of vulnerabilities, and continuous improvement of security measures. By continuously assessing vulnerabilities and making necessary improvements to security measures, organizations can stay ahead of potential cyber threats and better protect their systems and data. This ongoing effort to enhance cybersecurity measures is crucial in mitigating the impact and potential damages of cyberattacks, ensuring the integrity and confidentiality of sensitive information. Through continuous improvement of cybersecurity measures, organizations can effectively mitigate the impact and potential damages of cyberattacks, thereby ensuring the integrity and confidentiality of sensitive information. This ongoing commitment to cybersecurity is essential for organizations to maintain trust with their stakeholders and protect their reputations in an increasingly digital world. By demonstrating a strong commitment to cybersecurity, organizations can build trust with their stakeholders and protect their reputations in an increasingly digital world. This

commitment involves implementing robust cybersecurity measures and regularly assessing and improving security protocols to stay ahead of evolving cyber threats. By consistently implementing robust cybersecurity measures and regularly assessing and improving security protocols, organizations can stay ahead of evolving cyber threats and maintain their commitment to cybersecurity valavanis2024understanding.

2.1.8 SABSA Architecture Matrix Assessment

The SABSA Architecture Matrix is a tool used to assess how well an existing network or security architecture fits with the desired end-state SABSA model based on business requirements. This is achieved by comparing the "as-is" architecture with the "to-be" SABSA architecture, focusing on how the two link together. The matrix is discussed graphically by taking two views of the architecture: the first discussing the process areas in the form of a Swimlane diagram, and the second showing the specific points of data or application transfer with a mapping table (Sherwood, Clark, and Lynas, 2005).

The Sherwood Applied Business Security Architecture (SABSA) is a comprehensive framework that provides the tools to implement risk-driven enterprise information security and effectively address the related business risk. It is firmly based on a business-driven security strategy and encompasses security policies, processes, and technology to build an integrated set of enterprise security architectures. SABSA provides a methodology to link business objectives with security design and implementation, ensure consistent policy and risk management decisions, and enable cost-effective allocation of security resources. The SABSA architecture matrix assessment plays a crucial role in evaluating the effectiveness of existing security measures and identifying potential vulnerabilities within the system. It involves a systematic analysis of the organization's security architecture components

to prioritize and address any gaps or weaknesses in the system. By conducting the SABSA architecture matrix assessment, organizations can identify potential vulnerabilities and make informed decisions regarding allocating resources to strengthen their cybersecurity measures. This assessment helps organizations gain a comprehensive understanding of their security posture and enables them to develop effective strategies to reduce the risk of cyberattacks (Sherwood, Clark, and Lynas, 2005).

Furthermore, the SABSA architecture matrix assessment assists organizations in identifying the most critical areas for improvement in their cybersecurity governance, allowing them to prioritize and implement necessary measures to mitigate cyber threats. By conducting this assessment, organizations can enhance their overall cybersecurity posture and reduce the likelihood and impact of cyberattacks. This ultimately leads to a more secure and resilient digital infrastructure, safeguarding sensitive data and protecting against potential risks and threats. As a result, organizations can foster trust and confidence among stakeholders and ensure the continuity of their operations in an increasingly interconnected world. Additionally, the SABSA architecture matrix assessment provides organizations with a framework to monitor and continually improve their cybersecurity governance, allowing them to adapt to emerging threats and stay ahead of cyberattackers. This framework enables organizations to maintain an effective cybersecurity posture and optimize their security measures to address evolving cyber threats and challenges. The SABSA architecture matrix assessment serves as a crucial tool in achieving an ongoing and proactive approach to cybersecurity, ensuring that organizations can effectively mitigate cyber risks and protect their valuable assets. By regularly conducting this assessment, organizations can stay ahead of potential cyber threats, continuously improve their security measures, and safeguard their critical information and systems (Sherwood, Clark, and Lynas, 2005).

Moreover, the SABSA architecture matrix assessment enables organizations to demonstrate their commitment to cybersecurity governance, compliance with regulatory requirements, and adherence to industry best practices, further enhancing their reputation and credibility in the digital landscape. This assessment serves as tangible evidence that organizations have implemented robust security measures and are taking proactive steps to protect sensitive information and maintain the integrity of their systems. SABSA architecture matrix assessment is a vital component of cybersecurity governance, providing organizations with the means to evaluate and strengthen their security measures, prioritize resources, and demonstrate their commitment to protecting sensitive information in an increasingly interconnected world. By leveraging this assessment, organizations can enhance their overall cybersecurity resilience and effectively combat the ever-evolving landscape of cyber threats (Sherwood, Clark, and Lynas, 2005).

2.1.9 Maturity and Capability Measurement using CMMI

V2.0 Methodology

CMMI V2.0 (Capability Maturity Model Integration) is the latest version of the CMMI framework, released in 2018 by the CMMI Institute (now part of ISACA). It is designed to modernize process improvement across multiple disciplines, including cybersecurity, and help organizations improve their performance through a more flexible and streamlined approach. CMMI V2.0 builds on previous versions, with a greater emphasis on performance improvement, integrating agile methodologies, and making the framework more accessible and intuitive for organizations of all sizes (Institute, 2021).

The CMMI V2.0 framework offers a five-level maturity model:

- **Level 1 - Initial:** Processes are unpredictable and reactive. Success depends on individual effort.

- **Level 2 - Managed:** Processes are characterized for projects and are often reactive.
- **Level 3 - Defined:** Processes are proactive, well-documented, and standardized across the organization.
- **Level 4 - Quantitatively Managed:** Processes are measured and controlled with data-driven decision-making.
- **Level 5 - Optimizing:** Processes focus on continuous improvement through quantitative feedback, data, and innovation.

CMMI V2.0 strongly emphasizes aligning process improvement with business outcomes, integrating quantitative data and performance improvements to help organizations drive better results. High-maturity organizations using CMMI V2.0 have institutionalized process management, training, integrated teams, and other features that allow them to address complex risks and challenges more effectively. These organizations leverage CMMI V2.0 alongside other cybersecurity frameworks, such as COBIT 2019, NIST CSF v1. 1, and SABSA, to manage cybersecurity risks comprehensively.

2.1.9.1 Integration with Other Frameworks

The integration of CMMI V2.0 with COBIT 2019, NIST CSF v1. 1, and SABSA enhances the effectiveness of cybersecurity governance by providing a structured approach to maturity and capability measurement. CMMI V2.0 facilitates the measurement of organizational process maturity and capability, while COBIT 2019 focuses on governance and aligning IT processes with business objectives (*COBIT 2019 Framework*, 2018). NIST CSF v1. 1 introduces a risk-based approach to managing and mitigating cybersecurity risks (of Standards & Technology, 2018), and SABSA ensures that security measures are aligned with the business objectives (Sherwood, Clark, and Lynas, 2005).

The integration of these methodologies helps organizations to:

- **Improve Risk Management:** CMMI V2.0, alongside COBIT 2019, helps organizations implement governance models that ensure all cybersecurity risks are managed in line with the organization's strategic objectives. This integration improves the ability to identify, assess, and manage risks across the organization proactively.
- **Achieve Continuous Improvement:** CMMI V2.0's focus on continuous improvement, supported by quantitative data, complements NIST CSF v1.1's iterative approach to managing cybersecurity risks. Together, these frameworks help organizations continuously evaluate and refine their cybersecurity strategies to adapt to evolving threats.
- **Align Security with Business Goals:** SABSA ensures that all security initiatives are driven by real business needs. This approach is enhanced by CMMI V2.0's structured methodology, allowing better alignment between security efforts and business priorities, leading to stronger governance and operational outcomes.

2.1.9.2 Security and Defense in Depth

CMMI V2.0 is also integrated with security technologies such as CORAS (a model-based risk assessment tool) and methodologies like OWASP's attack patterns. This allows organizations to tailor their security initiatives and achieve a strong return on investment (ROI). One of the core strategies encouraged by CMMI V2.0 is the concept of *Defense in Depth*, which involves implementing multiple layers of security controls to safeguard an organization.

Defense in Depth ensures that if one layer of defense fails, other layers are still in place to prevent a full breach. Common layers include:

- **Network firewalls and intrusion detection systems (IDS):** These monitor and control network traffic to prevent unauthorized access.
- **Encryption:** Protects data from being accessed in transit or storage, even if intercepted.
- **Access Controls:** Implement strong authentication and authorization to limit access to sensitive data.
- **Regular Security Assessments:** Include continuous vulnerability assessments and penetration testing to identify and address potential weaknesses.

By integrating CMMI V2.0 with these layered security practices, organizations can incrementally develop and deploy more secure products and services. This strategy strengthens the overall security posture and reinforces the organization's commitment to protecting sensitive data and maintaining stakeholder trust.

2.1.9.3 Continuous Improvement in Cybersecurity Governance

CMMI V2.0's focus on continuous performance improvement ensures that organizations are well-equipped to adapt to emerging cybersecurity challenges. The framework integrates seamlessly with COBIT 2019, NIST CSF v1. 1, and SABSA, creating a continuous improvement model for cybersecurity governance. Organizations can leverage CMMI V2.0 to assess their current cybersecurity maturity, identify areas for improvement, and implement focused strategies to enhance their overall cybersecurity posture.

By measuring their maturity and capability over time, organizations using CMMI V2.0 can continuously improve their cybersecurity governance processes, ensuring they remain resilient against evolving threats.

The evolution of CMMI, from its initial focus on software development to its current application in cybersecurity governance, highlights the flexibility and adaptability of the framework. With the release of CMMI V2.0, organizations can now focus on performance improvement, integration with agile methodologies, and a streamlined approach to managing processes. When integrated with COBIT 2019, NIST CSF v1. 1, and SABSA, CMMI V2.0 provides a powerful framework for enhancing cybersecurity governance, improving risk management, and aligning cybersecurity efforts with business goals. This proactive approach is essential in today's rapidly evolving digital landscape, where organizations must remain vigilant against sophisticated cyber threats.

2.1.10 Identification of Key Gaps and Concerns

A significant gap identified is the lack of clear differentiation between cyber activities and conventional IT operations. Broad terms like "cybersecurity" and the growing trend of equating all IT-related risks with cyber risks lead to an implicit assumption that cyber activities are adequately addressed under the umbrella of general IT risk management. This lack of distinction results in cyber-specific risks being insufficiently controlled and managed, as organizations mistakenly believe that traditional IT risk management strategies are sufficient. A related issue is the limited focus on risk management techniques tailored specifically to cyber threats (Leszczyna, 2021).

(Darmi, Fernandez, Fathoni, & Wijayanto, 2024) research mentioned several key gaps in the body of knowledge concerning information security governance and the management of cyber activities were identified. The initial objective was to explore the existence and effectiveness of frameworks designed to govern and manage IT operations in a manner that specifically mitigates the risks posed by cyber threats. However, it became evident that there is a scarcity of literature explicitly addressing the governance of se-

curity activities as distinct from the broader governance of IT and information systems (IS) in general. From a cybersecurity governance perspective, the research highlights important strengths, particularly the use of well-established frameworks such as COBIT 2019, NIST CSF v1. 1, ISO/IEC 27002, and PCI DSS. The strength of COBIT 2019 lies in its ability to provide a comprehensive governance framework that aligns IT and business objectives. COBIT 2019 offers clear guidance on how organizations should structure their cybersecurity efforts in a way that enhances governance, risk management, and accountability across all IT functions. The inclusion of COBIT 2019 in the cited research reinforces the need for organizations to approach cybersecurity governance holistically, ensuring that cybersecurity is integrated into the broader governance processes.

According to (Möller, 2023) The integration of the NIST Cybersecurity Framework (CSF) is another strength of the research. NIST CSF v1. 1 provides a risk-based approach to identifying, protecting, detecting, responding to, and recovering from cyber threats. The cited research appropriately discusses how NIST CSF v1. 1 can be applied to improve risk management practices and enable organizations to build a more resilient cybersecurity posture. NIST CSF v1. 1's focus on continuous monitoring and adaptive security controls is essential in addressing the dynamic nature of cyber threats, and the research effectively highlights this.

Referring to (Kelley & Moyle, 2023), SABSA's role in aligning security with business requirements is also a strength of the research. SABSA provides an architecture framework that ensures cybersecurity efforts are strategically aligned with business goals and risk management. The research emphasizes the importance of using SABSA to ensure that security initiatives are not isolated but are embedded into the business architecture. The alignment of security controls with business processes is crucial in ensuring that cybersecurity governance is not treated as a standalone function

but is integral to business success. However, the cited research also has weaknesses. While it thoroughly discusses the SABSA framework, it does not sufficiently address the practical challenges organizations face in implementing it. For example, the research could benefit from a more detailed examination of how small to medium-sized enterprises (SMEs) can operationalize this framework, given their limited resources and expertise.

The research mentioned in this section lacks practical guidance on how these frameworks can be implemented cohesively. The research could be strengthened by providing more insights into how organizations can leverage the strengths of each framework in a complementary manner. For example, COBIT 2019 could provide the governance structure, while NIST CSF v1. 1 focuses on operational risk management, and SABSA ensures that security is integrated into the overall business architecture. Moreover, the research could explore how organizations of varying sizes and industries can adapt each framework to their specific needs. The practicalities of implementing these frameworks, especially in resource-constrained environments, need to be discussed in greater detail. Many organizations may find it challenging to fully adopt all aspects of these frameworks due to budget, staffing, or regulatory constraints. Therefore, the research could provide more actionable steps on how to prioritize and customize these frameworks based on organizational maturity, which could be evaluated using CMMI V2.0.

In conclusion, while the research cited provides a robust theoretical basis for cybersecurity governance, it would benefit from further exploration of practical implementation strategies. A more detailed discussion on the integration of COBIT 2019, NIST CSF v1. 1, and SABSA into a cohesive cybersecurity governance framework would make the research more actionable and applicable for organizations seeking to improve their cybersecurity posture.

2.1.11 Conclusion

In conclusion, chapter two has provided an extensive exploration of the cybersecurity governance landscape, covering studies conducted in the cybersecurity field. Each study contributes to this research, establishing a clear understanding of previous research and what they discovered until today. As the current research unfolds, the accrued benefits from these studies serve as guiding lights, furnishing valuable insights, methodologies, and tools. Positioned upon this robust foundation, the researcher is poised to advance the field, addressing contemporary challenges, and making a substantive contribution to the broader discourse on cybersecurity governance for a sustainable and secure digital future.

Chapter 3

Research Method

3.1 Research Method

This chapter outlines the research methodology, tools, and data collection techniques employed to investigate the effectiveness of the Cybersecurity Governance Framework in mitigating cyberattacks, focusing on critical infrastructure within Saudi Arabia. The research design ensures the reliability, validity, and applicability of the findings, providing a solid foundation for practical implementation. The chosen methodology is a mixed-methods approach, combining both qualitative and quantitative methods. This centers around a detailed case study exploring the integration of cybersecurity governance frameworks such as COBIT 2019, NIST CSF v1.1, and SABSA in a real-world organizational context.

The qualitative aspect focuses on understanding the organizational dynamics and governance practices, while the quantitative aspect evaluates cybersecurity maturity, risk profiles, and key performance indicators (KPIs).

The research approach and tools, such as the RACI matrix and Cybersecurity Governance Tool, provide profound insights into the organization's cybersecurity posture, risk management practices, and the effectiveness of implemented frameworks.

3.2 Methodology Used

This research employs a mixed-methods case study methodology to explore how integrating cybersecurity frameworks, particularly COBIT 2019, NIST CSF v1.1, and SABSA, can mitigate cybersecurity risks in a critical infrastructure organization in Saudi Arabia. This approach enables a detailed, context-specific investigation of how governance frameworks are applied in practice, allowing for both qualitative and quantitative data collection and analysis.

3.2.1 Research Purpose and Strategy

The primary purpose of this research is to evaluate how a comprehensive cybersecurity governance framework enhances the cybersecurity posture of critical infrastructure organizations in Saudi Arabia. This involves understanding both the technical aspects of cybersecurity and how organizational structures, governance, and risk management practices are optimized through the application of recognized frameworks.

3.2.1.1 Research Approach

A mixed-methods approach was chosen to integrate both qualitative and quantitative data for a more holistic understanding of the cybersecurity governance framework's impact. The qualitative case study provides in-depth insights into organizational practices and governance dynamics, while the

quantitative analysis allows for measurable evaluations of cybersecurity maturity, control effectiveness, and risk management.

3.2.1.2 Research Strategy

The strategy is primarily exploratory, aiming to understand how the practical application of cybersecurity frameworks impacts the organization's ability to mitigate cybersecurity risks. Data collected from interviews, workshops, and direct observations provided qualitative insights into the organization's cybersecurity maturity, identified control gaps, and evaluated the effectiveness of governance mechanisms. Meanwhile, quantitative data analysis was used to measure cybersecurity risk levels, maturity scores, and critical performance metrics.

3.2.2 Data Collection

The data collection process was carefully designed to capture both qualitative and quantitative data, providing a comprehensive view of the organization's cybersecurity governance and risk management practices.

3.2.2.1 Primary Data Collection

Primary data was collected through:

- **Interviews:** In-depth interviews with IT personnel, cybersecurity staff, and key executives provided insights into current cybersecurity practices, governance structures, and risk management approaches.
- **Workshops:** Over 25 workshops were held with key stakeholders, focusing on evaluating the organization's capability maturity levels, cybersecurity risk profiles, gaps, and solutions. These workshops were crucial in aligning organizational goals with COBIT 2019, NIST CSF v1.1, and SABSA.

- **Observations:** Direct observations were conducted on-site to assess how cybersecurity practices are implemented and managed within the organization's IT infrastructure. Observations included system configurations, security controls, and collaboration between departments.

3.2.2.2 Secondary Data Collection

Secondary data sources included:

- **Internal Documentation:** Over 50 internal documents, including IT policies, cybersecurity strategies, and security audit reports, were analyzed to provide a deeper understanding of the organization's current governance structure and risk management processes.
- **Benchmarking:** The organization's cybersecurity maturity was benchmarked against industry standards to identify areas of improvement, with a focus on compliance with national cybersecurity regulations, such as those set by the Saudi National Cybersecurity Authority (NCA).

3.2.2.3 Participant Selection Criteria

Participants were selected based on their roles within the organization's cybersecurity and IT departments. Demographic data, such as age, education level, and years of experience, were recorded to understand the diversity of perspectives influencing cybersecurity governance. Most participants were aged between 35 and 55, held IT-related bachelor's degrees, and had between 5 and 25 years of experience in the field.

3.2.3 Data Analysis

The data analysis process integrated both qualitative and quantitative methods to ensure a comprehensive understanding of the cybersecurity governance landscape and the effectiveness of the frameworks being applied.

3.2.3.1 Qualitative Data Analysis

Qualitative data from interviews, workshops, and observations was analyzed to explore the organizational context, decision-making processes, and collaboration dynamics. This analysis was critical in understanding the cultural and operational factors affecting cybersecurity governance.

3.2.3.2 Quantitative Data Analysis

The quantitative data analysis focused on cybersecurity metrics and maturity assessments:

- **Mapping NIST CSF v1.1 to COBIT 2019:** Each NIST CSF v1.1 subcategory was mapped to corresponding COBIT 2019 practices to identify how cybersecurity governance objectives aligned with the organization's cybersecurity framework.
- **Maturity Assessment Using CMMI V2.0:** The organization's capability maturity levels were assessed using CMMI V2.0, providing a quantitative evaluation of each control's effectiveness. Maturity scores were assigned to each cybersecurity domain, highlighting areas requiring improvement.
- **Gap Analysis:** Identified gaps were structured into recommendations using the SABSA architecture matrix, ensuring that both technical and governance aspects were addressed.
- **Statistical Analysis:** Quantitative data was analyzed using Excel-based tools to measure cybersecurity risk levels, calculate maturity scores, and monitor key performance indicators (KPIs). Statistical tools such as averages and IF functions were applied to assess the overall performance of the cybersecurity governance framework.

3.2.4 Research Tools

The research used several tools to assist in the implementation and assessment of the cybersecurity governance framework:

3.2.4.1 RACI Matrix and COBIT 2019

A **RACI matrix** (Responsible, Accountable, Consulted, Informed) was created based on the COBIT 2019 framework to assign clear roles and responsibilities within the cybersecurity governance structure. The use of the RACI matrix ensured that every stakeholder had defined roles, helping streamline decision-making and enhance accountability. This tool plays a crucial role in clarifying the responsibilities of IT and cybersecurity personnel in managing cybersecurity risks while aligning governance practices with business objectives.

Key Features of the RACI Matrix Tool:

1. **Role-Based Structure:** Each worksheet in the Excel tool corresponds to a specific role or committee within the organization, such as the *Chief Information Security Officer (CISO)*, *Chief Information Officer (CIO)*, *Board of Directors*, and the *Executive Committee*. This role-based structure ensures that responsibilities are well-defined across the organization.
2. **COBIT 2019 Activities:** The core sheet titled "*COBIT 2019 RACI*" lists governance and management objectives as defined by the COBIT 2019 framework. This includes tasks like risk management, compliance monitoring, IT operations, business continuity, and more. Each task is mapped to the relevant stakeholders using the RACI model.
3. **Cross-Functional Application:** The RACI matrix assigns roles across different levels of the organization, from executive management roles

like *Chief Executive Officer (CEO)*, *Chief Risk Officer (CRO)*, and *Chief Financial Officer (CFO)*, to specialized roles such as *Information Security Manager* and the *Project Management Office (PMO)*. This allows for shared responsibility across leadership and operational layers.

4. **Customization by Role:** Each role, such as the *CISO*, *CIO*, or *Project Manager*, has a dedicated sheet that shows the COBIT 2019 governance activities relevant to that particular role. Each sheet clearly designates the RACI assignment, such as marking the CISO as *Responsible (R)* for cybersecurity risk management, while the CIO may be *Accountable (A)* for ensuring strategic alignment with business goals.
5. **Comprehensive Governance Coverage:** The tool encompasses various governance functions, including information and technology (I&T), risk management, legal counsel, business continuity, and other essential processes. This ensures comprehensive coverage of all areas relevant to cybersecurity governance, adhering to the principles of COBIT 2019.
6. **Accountability and Transparency:** The matrix provides clear assignments for each role, fostering transparency and ensuring that every function knows their specific responsibilities. For example, the *Audit* and *Compliance* roles are often marked as *Consulted (C)* or *Informed (I)*, indicating their oversight role, while operational teams such as IT or security departments are typically marked as *Responsible (R)* for executing cybersecurity tasks.

Example of RACI Assignments:

- **Chief Information Security Officer (CISO):** In the "*Chief Information Security Officer*" sheet, the CISO is assigned as *Responsible (R)*

for various cybersecurity governance tasks, such as risk management, incident response, and ensuring compliance with IT governance standards.

- **Board of Directors:** The "*Board of Directors*" sheet marks the board as *Accountable (A)* for overseeing high-level cybersecurity governance, ensuring the organization's compliance with regulatory frameworks, and driving strategic cybersecurity initiatives.

This RACI matrix is an essential tool for assigning clear responsibilities and ensuring accountability in the implementation of cybersecurity governance. By mapping each role to specific governance activities within the COBIT 2019 framework, the organization can ensure that cybersecurity governance is integrated across all layers, from strategic leadership to operational execution.

3.2.4.2 COBIT 2019 Governance and Management Objectives, Practices, and Activities

The COBIT 2019 Governance and Management Objectives spreadsheet is a comprehensive tool used during the case study to map organizational objectives to governance practices and specific activities. This tool aids in aligning the cybersecurity governance framework with COBIT 2019 standards, ensuring that each objective is supported by actionable practices and tasks.

Key Features of the Spreadsheet:

1. **Objectives Sheet:** This sheet provides a list of high-level governance and management objectives. These objectives are aligned with the COBIT 2019 framework, which outlines goals for effective cybersecurity governance, risk management, IT operations, and compliance.

By defining clear objectives, the organization can focus its governance efforts on achieving critical outcomes, such as enhancing data protection and improving incident response times.

2. **Objectives-Practices Sheet:** The objectives are further mapped to specific governance and management practices in this sheet. Each objective is associated with one or more practical steps that must be followed to achieve it. This ensures that governance objectives are not just theoretical but are grounded in real-world actions. For example, a governance objective related to risk management may be mapped to practices such as continuous risk assessment, incident response planning, and compliance auditing.
3. **Activities Sheet:** This sheet lists detailed activities that correspond to each practice. The activities represent the actionable steps that need to be performed to fulfill governance practices. These activities include tasks such as conducting regular security audits, performing vulnerability assessments, ensuring compliance with cybersecurity regulations, and more. The detailed breakdown of activities allows for the granular tracking of how well governance practices are being implemented across the organization.

Practical Application in the Case Study: During the case study, the spreadsheet was used to ensure that every cybersecurity governance objective was supported by specific practices and activities. This allowed the organization to:

- Identify gaps between current governance practices and COBIT 2019 standards.
- Implement targeted activities to close gaps in governance, ensuring compliance with both internal policies and external regulations.

- Track the progress of governance initiatives by monitoring the completion of activities and the achievement of objectives.

By linking governance objectives to practices and specific activities, this tool provided a structured approach to enhancing cybersecurity governance and aligning the organization's IT operations with the best practices outlined in the COBIT 2019 framework.

3.2.4.3 COBIT 2019 Governance System Design Toolkit

The **COBIT 2019 Governance System Design Toolkit** is an Excel-based tool developed to help organizations customize and implement governance systems tailored to their specific needs. Based on COBIT 2019, the tool enables organizations to align their governance and management objectives with their enterprise goals by assessing and refining their governance scope across various domains. The tool uses a structured approach to assess the organization's current maturity level and define target levels, helping identify the areas of focus for governance improvement.

Key Components of the Toolkit: The toolkit consists of several key sheets, each contributing to a systematic design of the governance framework:

1. **Instructions Sheet:** The *Instructions* sheet provides users with the necessary guidelines to navigate and use the toolkit. It includes key definitions and explanations of terms used in COBIT 2019, such as relative importance, capability levels, and the process for refining the scope of governance and management objectives.
2. **Canvas Sheet:** The *Canvas* sheet is the central worksheet where users define the scope of their governance system. It guides users through the following steps:

- **Step 1:** Define the enterprise strategy and goals.
- **Step 2:** Determine the initial scope of governance objectives by aligning them with enterprise strategy and goals.
- **Step 3:** Adjust the governance scope based on various design factors (such as organizational size, risk profile, or technology adoption).
- **Step 4:** Conclude the governance scope by setting target capability levels and refining governance and management objectives.

The *Canvas* sheet also contains fields to document the suggested and agreed target capability levels for each governance and management objective.

3. **Design Factors Sheets (DF1 to DF10):** Each design factor sheet (e.g., *DF1*, *DF2*, *DF3*) corresponds to a specific element of the organization's environment that influences the governance system design. Examples of design factors include:

- **DF1 (Enterprise Strategy):** Helps align the governance objectives with the overall strategy of the organization.
- **DF5 (Risk Profile):** Ensures that governance decisions reflect the organization's risk appetite and tolerance.
- **DF7 (Threat Landscape):** Assesses external threats and their impact on governance priorities.

For each design factor, users assign relative importance to each governance objective and management activity. This relative importance helps refine the initial governance scope defined in the *Canvas* sheet.

4. **Mapping Sheets (e.g., DF1map, DF2map):** The mapping sheets are used to map the design factors (DF1 through DF10) to the relevant governance and management objectives. This mapping allows organizations to adjust governance priorities based on the contextual factors defined by each design factor. For example, if the organization's enterprise strategy places a strong emphasis on digital transformation, the relevant objectives in the *DF1map* sheet would be given higher importance.
5. **Dashboards (Dashboard1 and Dashboard2):** The dashboards provide a visual summary of the governance system design process. These sheets compile data from the *Canvas* and design factor sheets to present an overview of the organization's current and target capability levels. The dashboards are used to track progress and identify areas that require attention or further refinement.

How the Toolkit Works: The COBIT 2019 Governance System Design Toolkit is designed to be used in a step-by-step process that ensures alignment between an organization's governance objectives and its strategic goals. The process can be summarized as follows:

- **Step 1: Define Initial Governance Scope:** The organization begins by defining its enterprise strategy, goals, and related governance and management objectives in the *Canvas* sheet. Initial weights are assigned to each objective based on their alignment with enterprise goals.
- **Step 2: Apply Design Factors:** Using the design factor sheets (DF1 to DF10), the organization assesses how contextual factors like risk profile, threat landscape, and compliance requirements affect the importance of each governance objective. The tool automatically adjusts

the relative importance of each objective based on the inputs in the design factor sheets.

- **Step 3: Refine Governance Scope:** Once the design factors have been applied, the organization adjusts the governance scope to reflect the refined priorities. For example, if a high-risk profile is identified in *DF5*, certain governance objectives related to risk management may be assigned higher importance.
- **Step 4: Set Target Capability Levels:** For each governance objective, the organization sets target capability levels, which represent the desired maturity of governance practices. The current and target levels are displayed in the *Canvas* sheet, providing a clear view of the areas where improvement is needed.
- **Step 5: Monitor and Track Progress:** The dashboards compile all the inputs and adjustments made throughout the toolkit, providing a summary of the governance design process. These dashboards allow the organization to monitor progress, track the completion of activities, and ensure that governance objectives are being met.

Example of Toolkit Usage:

- **Enterprise Strategy Alignment (DF1):** If the organization's enterprise strategy emphasizes digital transformation, the *DF1* sheet would assign higher weights to objectives related to IT governance, innovation, and security. This ensures that governance activities prioritize digital capabilities.
- **Risk Profile Assessment (DF5):** For an organization with a high-risk appetite, the *DF5* sheet would increase the relative importance of risk management objectives, such as continuous risk monitoring and

incident response. These objectives would be assigned higher priority when refining the governance scope.

Benefits of the Toolkit:

- **Tailored Governance System:** The toolkit allows organizations to design governance systems that are fully aligned with their unique strategic goals, risk profiles, and external threats. This tailored approach ensures that governance efforts are relevant and impactful.
- **Data-Driven Decisions:** By applying design factors and mapping them to governance objectives, the toolkit enables data-driven decision-making. Organizations can prioritize objectives based on contextual factors rather than arbitrary decision-making.
- **Continuous Monitoring:** The dashboards provide real-time insights into the organization's governance progress, allowing for continuous monitoring and adjustment as needed.

This toolkit provides a robust framework for designing and refining governance systems according to COBIT 2019 standards. By following a structured process, organizations can ensure that their governance efforts are aligned with strategic goals and are capable of meeting both current and future challenges.

3.2.4.4 Cybersecurity Governance Tool

The **Cybersecurity Governance Tool** is an Excel-based assessment and monitoring tool designed to assist organizations in implementing, assessing, and tracking cybersecurity governance initiatives. This tool integrates best practices from the COBIT 2019, NIST CSF v1.1 (Cybersecurity Framework), and SABSA frameworks, offering a comprehensive evaluation of the

organization's cybersecurity posture. The tool is intended to be used on a quarterly basis or when significant organizational changes occur.

Key Components of the Tool: The Cybersecurity Governance Tool consists of four primary sheets, each with a specific function that supports assessing and improving the organization's cybersecurity governance framework:

1. **COBIT NIST CSF SABSA Assessment Sheet:** This sheet provides an integrated assessment of governance practices and cybersecurity controls using mappings between COBIT 2019, NIST CSF v1.1, and SABSA. The organization uses this sheet to evaluate its current cybersecurity posture by assessing which controls have been implemented and to what extent.

Example:

- For *ID.AM-1* (Asset Management: "Physical devices and systems within the organization are inventoried"), the tool maps this NIST CSF subcategory to COBIT 2019 practices *BAI09.01* and *BAI09.02*.
- The organization assesses the current status of implementation (e.g., partially implemented) and identifies gaps such as "Security Blind Spots" due to unclassified devices. Recommendations might include developing a more comprehensive asset inventory.

2. **CS Maturity & Capability Status Sheet:** This sheet tracks the organization's cybersecurity maturity and capability levels across various domains. It allows organizations to monitor progress toward their target maturity levels, providing a snapshot of current maturity and identifying areas where improvement is needed.

Example:

- If the maturity level of incident response is 2.0 (repeatable practices), the target maturity level might be set at 3.0 (defined and standardized processes). This sheet helps track the progress of moving from the current to the target level.

3. **CS Risk Register Sheet:** The Risk Register captures identified cybersecurity risks, describing their potential impact, inherent risk levels, residual risk levels after applying controls, and mitigation strategies.

Example:

- A risk associated with phishing attacks may be categorized with an inherent risk rating of "High." After implementing anti-phishing measures such as email filtering and employee training, the residual risk is recorded as "Medium."

4. **KPI (Key Performance Indicators) Sheet:** This sheet tracks and monitors the organization's cybersecurity performance. Each KPI measures specific aspects of cybersecurity operations, such as the number of incidents, response times, and the percentage of alerts addressed within a set timeframe.

Example:

- A KPI may track the percentage of critical security alerts addressed within 24 hours, with a target of 95%. The sheet tracks actual performance over different quarters and flags areas needing improvement.

How the Tool Functions: The Cybersecurity Governance Tool is designed to assess the organization's cybersecurity controls and governance across several dimensions:

1. **Mapping and Assessment:** The tool uses mappings of COBIT 2019 practices, NIST CSF v1.1 categories, and SABSA components to assess the current state of the organization's cybersecurity controls. For each mapped control, the implementation status, key gaps, and recommendations are evaluated.
2. **Maturity and Capability Tracking:** For each control, the organization assigns a maturity level (on a scale from 0 to 5) that represents the extent of implementation. The *CS Maturity & Capability Status* sheet helps track improvements over time and enables setting target maturity levels to drive governance efforts.
3. **Risk Monitoring:** The *CS Risk Register* tracks identified cybersecurity risks, capturing the inherent risks, residual risks, and the corresponding mitigation measures. This ensures that risk management remains a key focus of the organization's cybersecurity governance.
4. **Performance Monitoring:** The *KPI* sheet measures performance over time by tracking various metrics related to cybersecurity governance. The tool provides quarterly evaluations and allows organizations to monitor whether they are meeting their cybersecurity targets.

Examples of Tool Usage:

- **Assessment Example:**
 - The organization assesses its asset management controls under the *IDENTIFY (ID)* function. It finds that the inventory of physical devices is only partially implemented, which creates security blind spots. The current maturity is 2.0, and the recommendation is to implement a complete asset inventory system to remove unclassified devices.

- **Maturity Example:**

- The incident response process is assessed at a maturity level of 2.5. The organization sets a target maturity level of 3.5, which would require the establishment of standardized incident response procedures across the entire organization.

- **Risk Example:**

- A phishing attack risk is documented in the *Risk Register*. Initially, the inherent risk is categorized as "High." After applying training and email security measures, the residual risk is reduced to "Medium."

- **KPI Example:**

- The percentage of critical security alerts resolved within 24 hours is tracked as a key performance indicator (KPI). The target for Q1 is set at 90%, but the actual performance falls to 75%, prompting a review of the incident response process.

Benefits of the Tool:

- **Integrated Frameworks:** The tool integrates COBIT 2019, NIST CSF v1.1, and SABSA, providing a comprehensive assessment of cybersecurity governance and aligning best practices from multiple frameworks.
- **Continuous Improvement:** The tool is designed for quarterly assessments and ongoing monitoring, enabling organizations to track their progress and adapt to changes in their environment. It fosters a continuous improvement culture by tracking maturity levels and cybersecurity performance.

- **Risk-Focused Governance:** By including a detailed risk register, the tool ensures that organizations maintain a risk-based focus when managing their cybersecurity governance. The tool helps prioritize high-risk areas and monitor how well mitigation strategies are working.

The Cybersecurity Governance Tool provides an integrated approach to managing cybersecurity governance, ensuring that organizations can assess, monitor, and continuously improve their cybersecurity practices while remaining aligned with industry frameworks.

3.2.5 Conclusion

This chapter outlined the research methodology used in investigating the effectiveness of a cybersecurity governance framework within Saudi Arabia's critical infrastructure. By adopting a *mixed-methods case study approach*, the research explored the application of governance frameworks in a real-world context. The integration of multiple research tools, including the RACI matrix and the Cybersecurity Governance Tool, provided a structured approach to understanding the complexities of cybersecurity governance. Data analysis, both qualitative and quantitative, revealed key insights into the organization's cybersecurity maturity, risk management practices, and the practical challenges of implementing frameworks like COBIT 2019, NIST CSF v1.1, and SABSA.

By detailing the research approach, data collection methods, and tools, this chapter establishes a clear framework for how cybersecurity governance can be assessed and improved, offering a roadmap for future research and practical application in the region.

Chapter 4

Case Study Analysis

4.1 Case Study Analysis

In the realm of cybersecurity governance, the symbiotic relationship between theoretical frameworks and practical applications comes to the forefront in this pivotal chapter. Chapter Four intricately weaves the narrative of a comprehensive case study and the innovative implementation of a bespoke Cybersecurity Governance Tool. Together, they illuminate the nuances of organizational challenges, strategic decisions, and the path toward fortifying cybersecurity frameworks within the unique context of Saudi Arabia.

4.2 Case Study

4.2.1 Organization Alpha

The organization, anonymized for this research, operates as a large-sized company in the information technology industry with multiple subsidiaries. Specializing in technology products and IT services, it maintains partnerships with major global companies like Microsoft, Google, Amazon, etc. Catering to both government and private sectors, the information technology industry recognizes its critical infrastructure role, intensifying the need for a dependable cybersecurity posture due to regulatory requirements, partnerships, and customer expectations.

Aspiring to expand and become a publicly traded company, the enterprise faced challenges during the COVID-19 pandemic. Resource limitations altered their digital transition plan, prompting a swift move to the cloud and implementing a new system. This shift led to vulnerabilities in the IT infrastructure, exploited by cyber attackers, resulting in data compromise, financial loss, and reputational damage. Investigation revealed a lack of communication and visibility in the IT infrastructure, compelling the organization to address cybersecurity issues, adopt the Enterprise Governance of Information Technology (EGIT) approach, and manage significant risks and security.

4.2.2 Business Challenges

In the aftermath of multiple cyberattacks on the organization's information and technology, the need for a reliable framework like COBIT 2019 and NIST CSF v1. 1 becomes imperative to provide adequate governance and security to the IT infrastructure. Addressing current risks, control gaps, and improving the risk profile are paramount. Challenges faced by the organi-

zation include:

- **Delayed Incident Response:** Centralized decision-making processes may lead to delayed responses to cyber incidents, impacting the mitigation of security breaches.

- **Lack of Collaboration and IT Visibility:** Absence of collaboration between different business entities and the IT department results in a lack of visibility into the organization's overall IT landscape, hindering effective cybersecurity risk assessment and management.

- **Inadequate Involvement in Technology Purchases:** Centralized management may lead to technology purchases without sufficient input from the IT department, potentially resulting in duplicate or incompatible technologies.

- **Redundant and Inapplicable Technologies:** The IT infrastructure is burdened with duplicate or irrelevant technologies, leading to increased complexity, inefficiencies, and higher maintenance costs.
- **Inadequate Risk Management:** Centralized structure hampers enterprise-level risk management, highlighting the need for improved practices to address the potential impact of cyber threats.

- **Compliance and Auditing:** Annual auditing and compliance with national cybersecurity authority regulations are necessary to ensure that cybersecurity measures meet required standards.

- **Data Security Breach:** Successful cyber-attacks compromise the organization's data integrity and erode trust by leading to the loss of confidential customer, financial, and government information.

- **Financial Fraud via Phishing:** Falling victim to phishing email scams results in unauthorized fund transfers, leading to significant financial losses and potential reputational damage.

- **Internal Data Misuse:** Unauthorized internal access to confidential information exposes weaknesses in the organization's internal data access

controls and security protocols.

These challenges necessitate immediate attention and robust solutions to safeguard data, enhance cybersecurity measures, and streamline the organization's IT landscape for operational efficiency and resilience.

4.2.3 Data Collection Design

The methodology employed for gathering data in this case study aligns with a comprehensive approach aimed at capturing both quantitative and qualitative insights. The primary focus is on understanding the organization's cybersecurity posture, responsiveness to cyber threats, and its capacity to contain and manage cyber-attacks.

- **Quantitative Data Collection:**

- o **Security Metrics Analysis:** Utilizing existing security metrics and performance indicators to quantify aspects such as incident frequency, resolution times, and effectiveness of current security controls.

- **Qualitative Data Collection:**

- o **Interviews:** In-depth interviews with key stakeholders, including IT and cybersecurity personnel, to gather qualitative insights into the challenges faced, communication gaps, and perceptions regarding the current state of cybersecurity.

- o **Workshops:** Interactive sessions involving key personnel to facilitate discussions on specific cybersecurity issues, risk perceptions, and potential improvements.

- o **Observations:** Direct observations of the organization's IT infrastructure, cybersecurity practices, and collaboration dynamics to supplement and validate interview and workshop findings.

- **Mixed-Methods Integration:**

- o **Triangulation:** The convergence of quantitative and qualitative data to validate findings from different sources, enhancing the overall credibility

and reliability of the results.

- o Sequential Exploratory Strategy: Initial qualitative data collection informs the development of quantitative instruments, allowing for a more nuanced exploration of identified themes.

- o Sampling: Selection of participants based on their roles, responsibilities, and expertise in IT and cybersecurity to ensure representation from different organizational levels.

- o Time Frame: Data collection will span Aug 2022 until Sep 2023, providing a comprehensive snapshot of the organization's cybersecurity landscape during this period.

The chosen data collection design aims to generate a holistic understanding of the organization's cybersecurity challenges, strengths, and areas for improvement. This approach ensures that both quantitative metrics and qualitative insights are leveraged to provide a nuanced and comprehensive analysis of the organization's cybersecurity posture.

4.2.4 Assessment Findings

The initial assessment conducted on the selected organization aimed to investigate into various aspects of its IT and cybersecurity landscape. The findings provide crucial insights into the organization's current state and highlight areas that require attention and improvement.

- Risk Management Practices:

- o Identified gap: The organization lacks robust risk management practices, which contributes to vulnerabilities in addressing cybersecurity risks and compliance requirements.

- o Strategic goal: Implement a comprehensive risk management framework aligned with organizational objectives and regulatory requirements to proactively identify, assess, and mitigate cybersecurity risks.

- Centralized Decision-Making:

- o Identified gap: The centralized management approach impedes timely responses to cyber incidents and limits collaboration and visibility across business units and the IT department.

- o Strategic goal: Foster a culture of collaboration and transparency to enhance visibility into the organization's IT landscape and cybersecurity risks.

- Compliance and Auditing:

- o Identified gap: The organization requires annual auditing and needs to comply with national cybersecurity authority regulations to ensure its cybersecurity measures meet necessary standards.

- o Strategic goal: Establish processes and controls to ensure ongoing compliance with national cybersecurity authority regulations and proactively prepare for annual audits.

- Framework Implementation:

- o Identified gap: The organization needs to adopt and integrate frameworks such as the NIST Cybersecurity Framework, SABSA, and COBIT for structured management of cybersecurity risks and enterprise IT governance.

- o Strategic goal: Implement the recommended frameworks to enhance cybersecurity posture and governance practices.

- Response to Initial Assessment Questions:

- o IT/Cybersecurity Department Structure: The cybersecurity department reports to Information Technology under the Chief Information Officer (CIO).

- o Current IT/Cybersecurity Model: The organization follows a hybrid model with some services on-premises and others outsourced.

- o Number of IT/Cybersecurity Staff: A total of 30 employees, with 22 in IT and 8 in the Cybersecurity department.

- o Application of IT/Cybersecurity Governance: Cybersecurity Governance is applied based on the Saudi National Cybersecurity Authority (NCA) Essential Cybersecurity Controls and ISO 27001.

- o Cybersecurity Department Structure: Cybersecurity is integrated with Risk, Governance, Compliance (GRC), and Access Management, with cybersecurity operations outsourced to a local service provider.

- o Regulatory Compliance: Subject to NCA and SADIA regulations; preparing for Saudi Capital Market Authority (CMA) cybersecurity regulations due to plans to become a publicly traded company.

- o Responsibility for Cybersecurity: Cybersecurity is everyone's responsibility, with formal responsibilities distributed among IT, the cybersecurity team, and a managed service provider.

- o Chief Information Security Officer (CISO): No current CISO; actively interviewing candidates to fulfill Saudi Capital Market Authority requirements.

- o Cross-Departmental Meetings on Cybersecurity: Cybersecurity issues are raised during weekly management communication meetings.

- o Protection of Customer Information: Protection aligns with NCA, SDAIA, and ISO cybersecurity requirements.

These initial findings provide a foundation for further analysis, guiding the organization toward strategic goals that address gaps and enhance its overall cybersecurity posture, risk management practices, and governance framework.

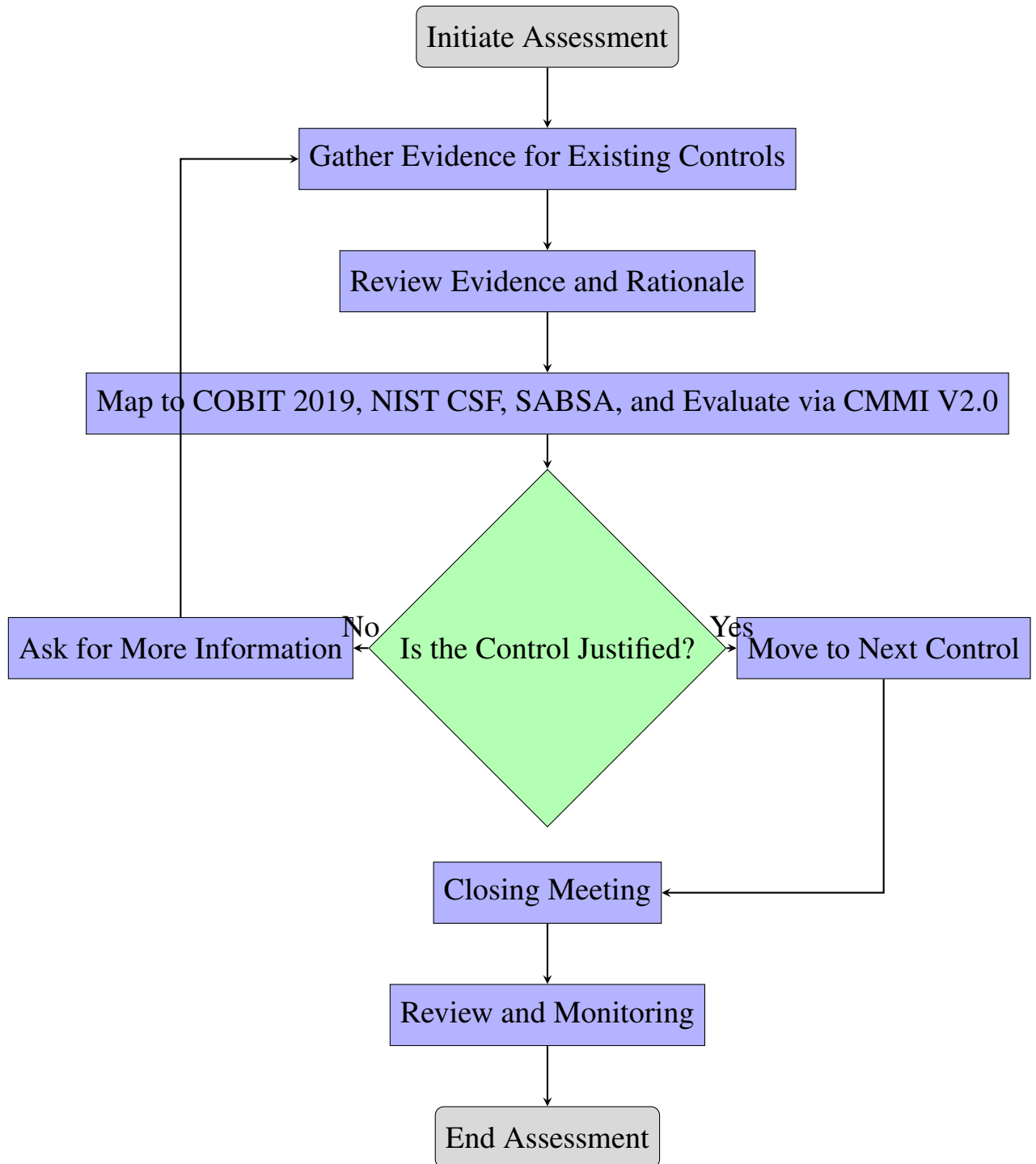
4.2.5 Current Cybersecurity Maturity and Incident Response

The selected organization currently demonstrates a cybersecurity maturity level of 1.3, according to the CMMI V2.0 framework, aligned with COBIT 2019, NIST CSF v1. 1, and SABSA. This maturity level reflects an organization in the early stages of cybersecurity governance, with ad-hoc or inconsistent practices, and limited capability for proactive threat manage-

ment. The assessment highlights several areas that require improvement to enhance the overall cybersecurity posture.

4.2.5.1 Cybersecurity Control Assessment Process

The following flowchart outlines the structured process for conducting a comprehensive cybersecurity control assessment. This process begins with the initiation of the assessment, followed by the collection and review of evidence related to existing controls. The gathered evidence is then mapped against recognized frameworks such as COBIT 2019, NIST CSF v1.1, and SABSA, and evaluated through the CMMI V2.0 model. A decision is made based on whether the controls are justified, leading either to further information gathering or progression to the next control in the assessment. The process concludes with a closing meeting, followed by continuous review and monitoring to ensure ongoing improvement. The iterative nature of this assessment ensures that it is revisited annually or in response to significant organizational changes, ensuring an evolving and resilient cybersecurity posture.



Repeat Assessment Annually or When Major Change Occurs

The cybersecurity control assessment process depicted above is designed to ensure thorough evaluation and continuous monitoring of the organization's cybersecurity posture. By aligning with established frameworks such

as COBIT 2019, NIST CSF v1.1, and SABSA and using the CMMI V2.0 evaluation model, this iterative process aims to enhance both governance and proactive threat management capabilities. The result is a refined approach that adapts to the organization's evolving needs and external cyber-security threats.

4.2.5.2 Incident Response Procedures for Common Cyberattacks (2020-2021)

The following table outlines Organization Alpha's Cybersecurity Incident Response Plan (CSIRP) actions for various types of attacks during 2020-2021, reflecting their lower cybersecurity maturity level of 1.3 and categorized incidents under each cyberattacks; also, by each phase of response: Issue Identification, Investigation, Recovery, and Reporting.

CSIRP Phase	Action	Status	Action Date
Malware			
Phase 1: Issue Identification	Detected via antivirus logs and suspicious file activity monitoring.	Complete	12/09/2020
Phase 2: Investigation	IT team isolates affected systems for in-depth analysis.	In Progress	12/11/2020
Phase 3: Recovery	Systems cleaned, patches applied, and vulnerabilities addressed.	Pending	12/01/2021
Phase 4: Reporting	Incident report submitted to senior management and NCA.	Pending	12/03/2021

System Compromise			
Phase 1: Issue Identification	Alert received from intrusion detection system (IDS).	Complete	05/11/2020
Phase 2: Investigation	Log analysis conducted to identify the compromised entry point.	In Progress	05/01/2021
Phase 3: Recovery	System restored from backup, vulnerabilities patched.	Pending	05/03/2021
Phase 4: Reporting	Findings shared with stakeholders and regulatory authorities.	Pending	05/05/2021
Denial of Service (DoS)			
Phase 1: Issue Identification	Network traffic analysis reveals high inbound traffic.	Complete	23/05/2021
Phase 2: Investigation	The cybersecurity team investigates traffic origins and characteristics.	In Progress	23/07/2021
Phase 3: Recovery	Traffic filtered, network throttling applied, and attackers blocked.	Pending	23/09/2021
Phase 4: Reporting	Report compiled for NCA and stakeholders.	Pending	23/11/2021

Personal/ Sensitive Data Breach			
Phase 1: Issue Identification	Detected through abnormal data access logs.	Complete	15/03/2020
Phase 2: Investigation	Data access and download logs reviewed to identify the breach scope.	In Progress	15/05/2020
Phase 3: Recovery	Access privileges revoked, affected systems reviewed for vulnerabilities.	Pending	15/07/2020
Phase 4: Reporting	Breach reported to customers, regulatory authorities, and NCA.	Pending	15/09/2020
Social Media Attacks			
Phase 1: Issue Identification	Alert from public relations team regarding unauthorized posts.	Complete	08/06/2020
Phase 2: Investigation	Social media accounts reviewed, access logs checked.	In Progress	08/08/2020
Phase 3: Recovery	Unauthorized posts removed, credentials reset.	Pending	08/10/2020

Phase 4: Re- porting	Internal and exter- nal communications released.	Pending	08/12/2020
Phishing At- tacks			
Phase 1: Issue Identification	Multiple users report suspicious emails.	Complete	10/10/2020
Phase 2: In- vestigation	The email headers and content are analyzed, sources blacklisted.	In Progress	10/12/2020
Phase 3: Re- covery	Affected accounts are secured, employees re- ceive training.	Pending	10/02/2021
Phase 4: Re- porting	Incident logged for se- nior management and stakeholders.	Pending	10/04/2021
Insider At- tacks			
Phase 1: Issue Identification	Unauthorized access patterns detected in the internal system.	Complete	21/08/2020
Phase 2: In- vestigation	User activity logs re- viewed, internal audit conducted.	In Progress	21/10/2020
Phase 3: Re- covery	User privileges re- voked, affected systems reviewed.	Pending	21/12/2020

Phase 4: Re-reporting	Detailed report provided to legal and human resources departments.	Pending	21/02/2021
Website Hacks			
Phase 1: Issue Identification	Web application firewall alerts unauthorized website access.	Complete	13/02/2021
Phase 2: Investigation	Logs reviewed, vulnerabilities identified in the website backend.	In Progress	13/04/2021
Phase 3: Recovery	Vulnerabilities patched, website restored to a secure state.	Pending	13/06/2021
Phase 4: Re-reporting	Incident reported to stakeholders and cybersecurity authority.	Pending	13/08/2021

4.2.5.3 Analysis of Incident Response

The table reflects the organization's low cybersecurity maturity level of 1.3 during 2020-2021, where incident response processes were slow and mostly reactive. The organization demonstrated significant delays in moving through the various phases of incident response, with response actions being ad-hoc and lacking formal processes. This highlights the need for a more structured, proactive approach to handling cyber incidents, with greater emphasis on monitoring, investigation protocols, and timely recovery.

4.2.6 Quantitative Cybersecurity Risks and Their Impact

In order to offer a more complete and quantitative understanding of the cybersecurity risks faced by Organization Alpha during the 2020-2021 period, a detailed risk assessment was conducted. This assessment focused on both the inherent risk (the level of risk before any controls or mitigation strategies were applied) and the residual risk (the level of risk after the implementation of security controls). The assessment provides insights into how these risks were managed and highlights areas requiring further attention.

4.2.6.1 Key Cybersecurity Risks Identified

The assessment identified several high-priority risks that posed significant challenges to the organization, particularly given its low cybersecurity maturity level of 1.3. Below is a summary of the main risks, their potential impacts, and the associated risk levels:

Risk Description	Impact	Inherent Risk (Pre-Control)	Residual Risk (Post- Control)
Lack of comprehensive Enterprise Architecture (EA)	Financial loss and business interruption	Medium	Low
IT operational infrastructure incidents due to misconfigurations	Business interruption, financial loss	Very High	Medium
Unauthorized actions by insiders	Reputational damage, business interruption	Very High	Low
Hardware failures due to insufficient testing	Financial loss and service downtime	High	Medium

Software failure due to improper testing and configuration	Business interruption, financial loss	High	Medium
Cybersecurity attack resulting from vulnerabilities in network security	Business interruption, reputational damage	Very High	High
Phishing attacks leading to data breaches	Reputational damage, financial loss	High	Moderate
Social media breaches causing unauthorized posts	Reputational damage	High	Low
Denial of Service (DoS) attacks affecting availability	Service downtime, financial loss	Very High	Moderate

4.2.6.2 Analysis of the Risk Data

The quantitative risk assessment reflects Organization Alpha's vulnerability during the 2020-2021 period. With a low maturity level, several risks, particularly those related to IT infrastructure, insider threats, and phishing attacks, posed serious threats. While the residual risk for many threats was reduced due to partial controls, significant gaps remained, particularly in areas like network security, where the residual risk remained high even after controls.

This analysis reinforces the need for a more robust cybersecurity governance framework, particularly the integration of COBIT 2019, NIST CSF v1. 1, and SABSA. Without structured governance and mature security practices, the organization was left vulnerable to significant business, financial, and reputational harm.

4.2.7 EGIT Program Implementation

The business case for the proposed EGIT program, rooted in the selected organization's context and based on COBIT 2019, serves as a strategic blueprint for managing risk and fortifying security. The primary goal is to enhance the overall governance of information and technology, ensuring a holistic and systematic approach. The imperative need for visibility into the organization's information and technology landscape underscores the significance of a successful EGIT implementation. Continuous monitoring of this business case becomes essential to guarantee a favorable outcome.

4.2.8 Scope Definition and Expansion

The EGIT program's scope is initially designed to encompass all impacted entities within the organization, aiming to effectively manage risk, security, and compliance with external requirements. Subsequently, this scope expands to include entities that have embraced digital transformation, ensuring the delivery of benefits and the continuity of operations.

4.2.9 Significance of EGIT Program Outcomes

The outcomes of the EGIT program bear immense importance for a multitude of internal and external stakeholders, ranging from the organization's board to government agencies. The challenges posed by the global connectivity, diverse subsidiaries, and critical infrastructure underline the pivotal role of the organization's information and technology infrastructure.

4.2.10 Strategic Approach and Stakeholder Engagement

For the successful execution of the EGIT program, the researcher will conduct multiple workshops. These workshops aim to identify relevant internal

and external stakeholders, establish the EGIT program team, and meticulously document responsibilities and accountabilities using the COBIT 2019 toolkit. Leveraging the COBIT 2019 management awareness diagnostic toolkit will aid in identifying governance and management objectives, practices, and activities for each entity. Prioritization of these objectives, considering IT-related business risk scenarios, is imperative.

4.2.11 Enhancing IT Process Capability

To ensure tangible business benefits for each business unit, there is a focus on increasing IT process capability to enhance efficiency and quality. This involves a concerted effort by each entity to reduce IT risks, necessitating the establishment of an EGIT program that ensures adequate governance coverage from a holistic perspective.

4.2.12 Capability and Maturity Assessment

Each business unit will establish a process for assessing capability and maturity levels using the Capability Maturity Model Integration V1.3 (CMMI). Regular self-assessments will become a standard practice, enabling units to define their levels and adjust objectives accordingly.

4.2.13 Five Sequential Phases Approach

The EGIT program unfolds in five sequential phases, each building upon the success of the previous one. The first phase involves the creation of a comprehensive action plan, categorizing activities, setting priorities using the Eisenhower Matrix, detailing resources, budgeting, and establishing timelines. Subsequent phases cover design, implementation, assessment, and monitoring with a focus on continuous improvement and alignment with

evolving enterprise goals.

4.2.14 Challenges and Stakeholder Approval

The initiation of the EGIT program's five sequential phases necessitates approval from the organization's corporate management. Given historical challenges in alignment, extensive discussions and explanations are anticipated to enhance communication and reporting. Establishing the EGIT program requires a dedicated budget and an extended timeline, demanding the collective commitment and awareness of all management levels.

4.2.15 First Phase: Comprehensive Action Plan for EGIT Program Implementation

Education and Awareness:

- Participants in the EGIT team will undergo the COBIT 2019 Foundation Course, establishing a structured understanding of COBIT 2019, NIST CSF v1. 1, and SABSA frameworks.
- Key Benefits of COBIT 2019 and CMMI V2.0 include building a comprehensive I and T framework, establishing a common language, and governing the latest framework updates.
- Key Benefits of NIST CSF v1. 1 encompass alignment with industry standards, adoption of cybersecurity controls, and enabling organizational resilience.
- Key Benefits of SABSA involve aligning security controls with business objectives and tailoring controls to the organization's architecture and needs.

Building Team Structure: Utilize the COBIT 2019 toolkit and an Excel-based RACI matrix to structure the EGIT team, fostering a shared understanding and language for effective governance.

Workshops with EGIT Team and Stakeholders: Conduct workshops with key stakeholders, including executive management, IT, cybersecurity, business unit management,

and audit/compliance teams. Detailed workshop information is available in Appendices.

Prioritization of Stakeholder Needs: • Internal Stakeholders (Board members and managers) seek resource optimization, reputation enhancement, and business growth.

• External Stakeholders (Customers and Regulators) require reliable, secure IT resources and mandate compliance with cybersecurity requirements.

Establish Communication Channels: • Form a steering committee as the primary communication channel, providing weekly status report updates, biweekly meetings, awareness campaigns, etc.

• Create Cybersecurity Steering Committee (CSC) structures following COBIT 2019 and NCA ECC recommendations. Refer to Appendices.

Organization Communication Plan:

• Select applicable COBIT 2019 guidance aligned with enterprise goals. For this case the selected enterprise goals with (P) primary will be used as to identify the alignment goals as per the COBIT® 2019 Framework: Governance and Management Objectives:

o AG01 I and T compliance and support for business compliance with external laws and regulations

o AG02 Managed I and T-related risk

o AG03 Realized benefits from I and T enabled investments and services portfolio

o AG04 Quality of technology related financial Information

o AG07 Security of information, processing infrastructure and applications, and privacy

o AG08 Enabling and supporting business processes by integrating applications and technology

o AG09 Delivering programs on time, on budget and meeting requirements and quality standards

o AG11 I and T compliance with internal policies

• Map selected primary alignment goals with governance and management objectives, focusing on priority objectives.

The P prime priority governance and management objectives based on the relevant selected there are alignment goals:

o EDM01 Ensured governance framework setting and maintenance

- o EDM02 Ensured benefits delivery
- o EDM03 Ensured risk optimization
- o EDM04 Ensured resource optimization
- o APO01 Managed I and T management framework
- o APO06 Managed budget and Costs
- o APO12 Managed risk
- o APO13 Managed security
- o BAI05 Managed organizational change
- o BAI09 Managed assets
- o BAI11 Managed projects
- o DSS04 Managed continuity
- o DSS05 Managed security services
- o MEA03 Managed compliance with external requirements
- o MEA04 Managed assurance

Although only the primary goals were selected, the result showed a lot of goals and objectives; therefore, they will be classified and divided into the roadmap of three years along with the strategy. After identifying the enterprise goals, alignment goals, and governance and management objectives as presented in the tables above. The next step is to select enterprise and alignment goals and metrics referring to the COBIT® 2019

Framework: Governance and Management Objectives:

2022						
Parameter	Current Capability Level		Target Capability Level		Gap	Action plan to fill gap
Evaluate, Direct and Monitor (EDM)	EDM	0.57	EDM	2.91	Lack of governance caused chaos in I&T that led to weekends in the IT infrastructure being exploited. Also, there is a lack of transparency due to the absence of the ability to oversee I&T processes, lack of engagement with the enterprise's stakeholders.	Provide a consistent approach integrated and aligned with the enterprise governance approach. I&T-related decisions are made in line with the enterprise's strategies and objectives, and the desired value is realized. Ensure I&T-related processes are overseen effectively and transparently, compliance with legal, contractual, and regulatory requirements is confirmed, and the governance requirements for board members are met.
EDM01 Ensured Governance Framework Setting and Maintenance	EDM01	0.50	EDM01	2.83		
EDM02 Ensured Benefits Delivery	EDM02	0.33	EDM02	3.11		
EDM03 Ensured Risk Optimization	EDM03	0.43	EDM03	2.71		
EDM04 Ensured Resource Optimization	EDM04	1.00	EDM04	3.00		
Align, Plan and Organize (APO)	APO	0.53	APO	3.24	Deficiency in the enterprise I&T management system that does not cover all the governance components. Also, lack of communication between the enterprise stakeholders and IT. Deficient integration between management of I&T-related enterprise risk with overall enterprise risk management (ERM). Inadequate cybersecurity controls to prevent or contain security incidents.	Implement a consistent management approach for enterprise governance requirements to be met, covering governance components. Foster a partnership between IT and enterprise stakeholders to enable efficient use of I&T-related resources and provide transparency. Integrate the management of I&T-related enterprise risk with overall enterprise risk management (ERM). Keep the impact and occurrence of information security incidents within the enterprise's risk appetite levels.
APO01 Managed I&T Management Framework	APO01	0.50	APO01	2.95		
APO06 Managed Budget and Costs	APO06	0.97	APO06	3.21		
APO12 Managed Risk	APO12	0.65	APO12	3.18		
APO13 Managed Security	APO13	0.00	APO13	3.60		
Build, Acquire and Implement (BAI)	BAI	0.60	BAI	3.07	Lack of commitment from the stakeholders during the business change results in an increase in the risk of failure. No visibility on all I&T assets causes issues and reduces the ability to optimize their value. Inadequate project management mechanism and lack of oversight of the project during all timeline status.	Prepare and commit stakeholders for business change and reduce the risk of failure. Account for all I&T assets and optimize the value provided by their use. Realize defined project outcomes and reduce the risk of unexpected delays, costs, and value erosion by improving communications to and involvement of business and end users.
BAI05 Managed Organizational Change	BAI05	0.33	BAI05	3.13		
BAI09 Managed Assets	BAI09	1.18	BAI09	3.31		
BAI11 Managed Projects	BAI11	0.28	BAI11	2.78		
Deliver, Service and Support (DSS)	DSS	0.62	DSS	4.30	The absence of business continuity leads to business operation disruption. Lack of security controls to prevent unauthorized access to data based on need-to-know.	Adapt rapidly, continue business operations, and maintain availability of resources and information at a level acceptable to the enterprise in the event of a significant disruption. Minimize the business impact of operational information security vulnerabilities and incidents.
DSS04 Managed Continuity	DSS04	0.13	DSS04	5.88		
DSS05 Managed Security Services	DSS05	1.12	DSS05	2.72		
Monitor, Evaluate and Assess (MEA)	MEA	0.50	MEA	2.89	Non-compliance with the external requirements like the NCA, etc. Lack of assurance initiatives that comply with internal requirements.	Ensure that the enterprise is compliant with all applicable external requirements. Develop efficient and effective assurance initiatives, providing guidance on planning, scoping, executing, and following up on assurance reviews, using a road map based on well-accepted assurance approaches.
MEA03 Managed Compliance With External Requirements	MEA03	0.89	MEA03	3.22		
MEA04 Managed Assurance	MEA04	0.12	MEA04	2.56		

Figure 4.1: Selected enterprise and alignment goals and metrics referring to the COBIT® 2019 Framework: Governance and Management Objectives.

- Identify enterprise and alignment goals, metrics, and develop a three-year roadmap along with the strategy.
- Classify and divide 521 identified activities into essential, important, and supportive categories based on the Eisenhower Matrix.

Environment Setup:

- Conclude this phase by creating an environment supportive of EGIT implementation, with top management providing direction, support, and oversight.
- Ensure key stakeholders are actively involved and have defined roles and responsibilities documented in the RACI matrix Excel.
- Establish the Cybersecurity Steering Committee (CSC) to create communication channels, KPIs, and KRIs for key stakeholders, enhancing visibility into EGIT and cybersecurity status.

4.2.16 Second Phase: Design of EGIT Program Implementation

Objective:

In the second phase, the researcher will tailor the governance system for the organization's enterprise information and technology (I and T), with a primary focus on cybersecurity. This phase involves customizing processes, organizational structures, information flows, and behaviors based on COBIT 2019 guidance.

Design Factors:

- Enterprise Strategy:
 - o Primary Strategy: Client Service Stability
 - o Secondary Strategy: Growth
- Enterprise Goals (Selected in Phase 1):
 - o EG02 Managed business risk
 - o EG03 Compliance with external laws and regulations
 - o EG05 Customer-oriented service culture
 - o EG08 Optimization of internal business process functionality
 - o EG09 Optimization of business process costs
 - o EG12 Managed digital transformation programs
 - o EG01 Portfolio of competitive products and services
 - o EG04 Quality of financial information
 - o EG11 Compliance with internal policies
- Risk Profile: Identified I and T-related risks and scenarios categorized based on COBIT 2019 framework.
- I and T-related Issues: Identified issues including frustration between business departments and IT, significant IT-related incidents, failures to meet regulatory requirements, and more.
- Threat Landscape: Operating in a high-threat environment due to geopolitical situation, industry sector, and business profile.
- Compliance Requirements: Subject to regular compliance requirements common across different industries.
- Role of IT: Classified as a Factory, where IT has an immediate impact on business processes and services.
- Sourcing Model for IT: Adopting a Hybrid model, combining Outsourcing, Cloud, and Insourced models.
- IT Implementation Methods: Following a Hybrid approach, combining traditional and modern IT implementation (bimodal IT).

- **Technology Adoption Strategy:** Being a Follower, waiting for new technologies to become mainstream and proven before adopting them.
- **Enterprise Size:** Categorized as a Large enterprise with more than 6,000 to 10,000 full-time employees.

Impact of Design Factors:

- **Prioritize Selected Management Objectives:** Top priorities include EDM03 Ensured risk optimization, APO12 Managed risk, APO13 Managed security, and DSS05 Managed security services.
- **Components Variation:** Completion of components from Phase 1 governance and management objectives excel sheet, especially focusing on documentation (policy, standard, procedure, process, etc.).
- **Need for Specific Focus Area Guidance:** Developing NIST CSF v1. 1 and SABSA approach along with COBIT, emphasizing the importance of cybersecurity controls.
- **Designing a Tailored Governance System:** Utilizing COBIT Design Guide toolkit, an Excel-based tool, to tailor the organization's strategy, goals, and objectives.

Steps in Design:

- **Understand the Enterprise Strategy:** Selecting primary and secondary archetypes based on the organization's focus on providing stable IT services and future growth.
- **Determine the Initial Scope of the Governance System:** Considering enterprise goals, risk profile, current I and T-related issues, and threat landscape to identify the initial scope.
- **Refine the Scope of the Governance System:** Considering the Threat Landscape (Design Factor 5) and adjusting the focus based on priority governance and management objectives.
- **Conclusion of Governance System Design:** Concluding the I and T governance system design to cover prioritized objectives with reasonable target capability levels and addressing critical lacks in capability. Attachments: Detailed assessment in the Excel sheet (Refer to Appendices).

4.2.17 Third and Fourth Phases Program Implementation and Assessment:

In this phase, the systematic implementation of COBIT 2019, NIST CSF v1. 1, and SABSA will be carried out. The implementation aims to cover cybersecurity governance and map security controls to governance and management objectives. The Cybersecurity Governance tool Excel will serve as a centralized location for both COBIT 2019 and NIST CSF v1. 1, facilitating the organization's implementation efforts.

COBIT 2019 and NIST CSF v1. 1 implementation stages:

- COBIT 2019: Phase 1—What Are the Drivers? The organization's decision to implement COBIT 2019, NIST CSF v1. 1, and SABSA is driven by the imperative to reduce cybersecurity risk and protect their IT. Key drivers include the need for stability in client services, growth challenges due to cybersecurity incidents, and the overarching goal of providing sustainable business growth. Challenges in this phase involve determining the benefits and value, rooted in communication gaps, unclear time frames, and unrealized benefits. Success factors include involving stakeholders through the CSC Committee, using a common language, and creating a sense of urgency.

- o NIST CSF v1. 1: Step 1: Prioritize and Scope: Aligning with the organization's mission to provide innovative, high-quality IT products, services, and solutions, NIST CSF v1. 1's first step involves prioritizing and scoping cybersecurity efforts. The scope covers all information and technologies within the organization's IT infrastructure, excluding third-party and partnership products. Compliance requirements are defined by the NCA ECC, and the organization analyzes its environment using the Cybersecurity Governance tool Excel.

- COBIT 2019: Phase 2—Where Are We Now? This phase aligns I and T-related objectives with enterprise strategies and addresses associated risks. COBIT objectives, assessed in phases one and two, are further analyzed using the Cybersecurity Governance tool Excel. Challenges include weak current enterprise governance, stemming from inadequate enterprise risk management. Success factors emphasize the application of risk management across the enterprise, with a change enablement strategy focused on forming a powerful guiding coalition.

- o NIST CSF v1. 1: Steps 2 and 3: Orient and Create a Current Profile: The organization's cybersecurity scope is deepened by orienting towards selected assets and systems,

while a current profile is created, detailing the state of cybersecurity risk management. Initial assessments highlight areas for improvement, with subsequent assessments showing advancements, adopting NCA Cybersecurity Risk Management Policy and enhancing risk management processes.

- COBIT 2019: Phase 3—Where Do We Want to Be? Setting realistic expectations and determining target maturity levels constitute this phase. Quick-win gap remediation activities are identified, prioritized based on benefit and complexity, and classified as essential, important, or supportive initiatives. Challenges involve communication gaps between IT and the business, rooted in inappropriate communication methods. Success factors stress using correct language and creating a clear vision, with change enablement focusing on communicating the vision.

- o NIST CSF v1. 1: Step 4: Conduct a Risk Assessment: The organization conducts a cybersecurity risk assessment following NCA procedures, using results to populate the CS Risk Register in the Cybersecurity Governance tool Excel. Current cyber threats are sourced from NCA alerts.

- o NIST CSF v1. 1: Step 5: Create a Target Profile: Benchmarking against global and local IT organizations, the organization assesses its cybersecurity maturity. Initial assessments below global industry standards improve over time, demonstrating the effectiveness of implemented initiatives.

- COBIT 2019: Phase 4—What Needs to Be Done? This phase involves creating a practical plan with justifiable business cases, monitored through project governance within the CSC Committee. Challenges include dealing with various levels of complexity, attributed to technical, organizational, and operating model complexities. Success factors emphasize prioritizing business priorities during implementation, with change enablement focusing on communicating the vision.

- o NIST CSF v1. 1: Step 6: Determine, Analyze, and Prioritize Gaps: Gap assessments are conducted using the Cybersecurity Governance tool Excel, leveraging CMMI V2.0 for measurement. Initiatives address gaps, incorporating activities recommended by COBIT, NIST CSF v1. 1, and SABSA. Quick wins include adopting NCA ECC and documenting policies using NCA toolkit.

- COBIT 2019: Phase 5—How Do We Get There? Utilizing proposed solutions from COBIT 2019, NIST CSF v1. 1, and SABSA, the organization integrates them into day-to-day practices. Weekly status updates, measured against KPIs in the Cybersecurity Governance tool Excel, provide visibility. Challenges include a lack of required skills and com-

petencies, emphasizing the need for change enablement planning. Success factors focus on cross-skilling, training, coaching, and mentoring.

- o NIST CSF v1. 1: Step 7: Implement Action Plan: The action plan, addressing each gap under cybersecurity domains, is monitored for implementation. Follow-up assessments trigger reassessment and continuous improvement action plans.

- COBIT 2019: Phase 6—Did We Get There? Implementing governance and management practices into daily operations requires a smooth transition. Challenges include potential failure to adopt or apply improvements, rooted in a poor understanding of new processes or tools. Success factors emphasize matching roles to individual capabilities and creating short-term wins.

- COBIT 2019: Phase 7—How Do We Keep the Momentum Going? Continual improvement and overall success lead to the realization of governance system benefits. Challenges involve maintaining interest and momentum, mitigated by regular communication and reinforcement of the need for robust services. Success factors include consolidating improvements and institutionalizing new approaches.

4.2.18 Fifth Phase Monitoring and Enhancement:

Continual improvement, change enablement, and program management form the core EGIT continual improvement life cycle. A comprehensive cybersecurity maturity and capability assessment by a third party, benchmarking against industry standards, and internal audits ensure ongoing compliance and improvement. The Cybersecurity Governance tool Excel serves as a checkpoint, providing a comprehensive view of status and progress. The organization adopts a continual improvement life cycle approach, ensuring perpetual enhancement of their EGIT system based on COBIT 2019 recommendations.

In conclusion, the EGIT program implementation, spanning across the five comprehensive phases guided by COBIT 2019, NIST CSF v1. 1, and SABSA, has been a strategic journey towards enhancing cybersecurity governance and fortifying the organization's information and technology landscape.

The initial phases, driven by a need to address cybersecurity risks and align with enterprise strategies, set the foundation for a robust governance system. Challenges such as communication gaps, unclear time frames, and unrealized benefits were met with proactive measures, including stakeholder involvement through the CSC Committee and a focus on creating a sense of urgency.

As the program progressed, each phase tackled specific objectives, from scoping and prioritizing cybersecurity efforts to conducting risk assessments and creating target profiles. Challenges such as communication gaps between IT and the business were addressed through clear vision creation, language adaptation, and effective change enablement strategies.

The fourth phase investigates practical planning and gap analysis, introducing project governance within the CSC Committee to monitor progress and address various complexities. Success factors emphasized prioritizing business needs, effective communication, and fostering a shared vision.

The fifth phase, focusing on implementation and continuous improvement, brought forth challenges related to skill gaps and competencies, addressed through change enablement strategies such as cross-skilling, training, and coaching. The organization utilized proposed solutions from COBIT 2019, NIST CSF v1. 1, and SABSA, integrating them into daily practices and ensuring regular monitoring through the Cybersecurity Governance tool Excel.

As the program reached its culmination in the seventh phase, the organization successfully embedded governance and management practices into daily operations, fostering a cybersecurity culture. Challenges of maintaining momentum were mitigated by regular communication and reinforcement of the need for robust services. The Cybersecurity Governance tool Excel served as a checkpoint, providing a comprehensive view of status and progress over time.

The fifth phase, focused on monitoring and enhancement, embraces a continual improvement life cycle, ensuring that the organization consistently evolves its EGIT system. A third-party cybersecurity maturity assessment, benchmarking against industry standards, and internal audits contribute to ongoing compliance and improvement.

In essence, the EGIT program's journey exemplifies a strategic and systematic approach to cybersecurity governance, culminating in a resilient and adaptable framework that not only mitigates risks but also positions the organization for sustained growth and success in the dynamic landscape of information and technology.

4.2.19 Cybersecurity Governance Tool:

The Cybersecurity Governance Tool is a robust solution encompassing a comprehensive set of cybersecurity requirements and controls. Tailored for organizations of all sizes, it facili-

tates the governance of cybersecurity implementations, considering the dynamic nature of the cybersecurity domain. The tool is designed to achieve the following objectives:

- o Rapidly Exploit Opportunities: Facilitate the organization in seizing new opportunities while maintaining cyber risk within acceptable limits.

- o Efficiently Respond to Threats: Enable the organization to respond to cyber threats without disrupting core business operations and minimize potential damages.

- o Regulatory Compliance: Assist the organization in complying with regulatory requirements and adopting global standards such as NIST, CIS, among others. This tool presents business-oriented cybersecurity domains with practical frameworks, delivering up-to-date best practices that can be seamlessly integrated into organizational programs, corporate policies, and business processes. The tool is easily updatable by organizations to align with the latest developments in the international cybersecurity landscape, ensuring coverage of evolving cyber threats.

Introduction

The Cybersecurity Governance Tool, implemented using Microsoft Excel, consolidates diverse resources for evaluating and assessing comprehensive cybersecurity controls. The tool was developed in 2022 and leverages extensive sources, including:

- Research into Top Cybersecurity Topics: In-depth exploration of trends in cybersecurity, cybersecurity governance, cyber threats, cyber-attacks, extinction-level cyber-attacks, cyber risks, risk assessment, and cyber insurance.

- Analysis of International Developments: Evaluation of cybersecurity standards and frameworks, including NIST Cybersecurity Framework, SABSA, COBIT 2019, etc.

- Benchmarking with Applied Cybersecurity Controls: Comparison of findings and results with cybersecurity controls applied in 2022 and 2023.

- Expert Input: Collaboration with experts through workshops, online interactions, face-to-face meetings, etc.

- Case Study in Saudi Arabia: Examination of the tool's effectiveness and deliverables through a case study conducted in Saudi Arabia.

Methodology for Tool Development

Utilizing Microsoft Excel sheets, the tool maps NIST CSF v1.1 functions, categories, subcategories, COBIT 2019 practices, current profiles (including implementation status and organizational practices), maturity and capacity levels in 2022, key gaps and concerns, recommendations, and best practices. The SABSA Matrix is employed to enhance the

tool's comprehensiveness.

Key Components and Features

The Cybersecurity Governance Tool consists of the following components:

- COBIT, NIST CSF v1. 1, and SABSA Assessment Sheet: Evaluates the organization's adherence to COBIT, NIST CSF v1. 1, and SABSA frameworks.
- Progress Sheet: Monitors the progress of cybersecurity implementations and assesses current status.
- CS Maturity and Capability Status Sheet: Assesses the maturity and capability status of the organization's cybersecurity practices.
- CS Risk Register Sheet: Identifies and registers cybersecurity risks within the organization.
- KPI Sheet: Measures Key Performance Indicators related to cybersecurity governance.

This tool was applied during proposed solutions for the case study, and a follow-up was conducted after a year to validate its value and effectiveness in managing cybersecurity controls and risks within the organization.

Case Study: Application of the Cybersecurity Governance Tool

In the application of the Cybersecurity Governance Tool to the selected organization, a meticulous process was undertaken to integrate the tool seamlessly into the case study. The following steps delineate the effective utilization of the tool within the organizational context:

Integration of the Tool in the Case Study

The Cybersecurity Governance Tool was systematically integrated into the case study process, aligning with the specific needs and challenges faced by the organization. This involved a tailored approach to implementing the tool's components, including the COBIT, NIST CSF v1. 1, and SABSA Assessment Sheet, Progress Sheet, CS Maturity and Capability Status Sheet, CS Risk Register Sheet, and KPI Sheet. Each component was strategically applied to evaluate and enhance the organization's cybersecurity posture.

Data Output and Analysis

The results generated by the Cybersecurity Governance Tool were meticulously analyzed, providing valuable insights into the organization's cybersecurity landscape. Data outputs from each component were scrutinized to understand the organization's adherence

to cybersecurity frameworks, progress in implementation, maturity and capability levels, identified risks, and key performance indicators. This comprehensive analysis facilitated a detailed understanding of the organization's strengths, weaknesses, and areas for improvement.

The application of the Cybersecurity Governance Tool unearthed nuanced insights into the organization's cybersecurity governance. It revealed areas where the organization excelled in aligning with established frameworks and practices, as well as areas that required attention and enhancement. The tool's effectiveness in providing a holistic view of the organization's cybersecurity controls and risk management practices was evident, contributing to a thorough understanding of the organization's cyber resilience.

Based on the findings from the tool application, specific adaptations and recommendations were formulated. These recommendations were tailored to address identified gaps, enhance cybersecurity controls, and optimize risk management strategies. The organization was provided with actionable insights to fortify its cybersecurity posture, ensuring alignment with global standards and regulations.

The application of the Cybersecurity Governance Tool in the case study not only served as a diagnostic instrument but also as a strategic guide for the organization to navigate the complexities of cybersecurity governance. The insights garnered from the tool's application played a pivotal role in shaping subsequent recommendations and interventions aimed at bolstering the organization's cyber resilience.

Discussion: Synthesis of Case Study and Tool Analysis The interplay between the case study findings and the analysis facilitated by the Cybersecurity Governance Tool reveals a symbiotic relationship that enhances the depth and breadth of understanding. The case study, enriched by real-world scenarios and organizational intricacies, provided context-specific insights. Simultaneously, the tool's analytical capabilities offered a systematic and structured evaluation, ensuring a comprehensive examination of the organization's cybersecurity landscape.

The integration of qualitative observations from the case study with quantitative data outputs from the tool presented a cohesive narrative, enriching the overall analysis.

Tool Effectiveness and Practical Implications

The effectiveness of the Cybersecurity Governance Tool became evident through its ability to distill complex cybersecurity governance issues into actionable insights. The practical implications derived from the tool's analysis enabled the organization to make informed decisions concerning its cybersecurity posture. The tool not only identified areas

of improvement but also served as a strategic guide for implementing practical solutions. This synthesis of case study and tool analysis reinforced the notion that a holistic approach, combining qualitative and quantitative methodologies, is paramount for a nuanced understanding of cybersecurity governance dynamics.

Recommendations: Bridging Case Study Insights and Tool Improvements

The procedural recommendations stemming from the synthesis of case study insights and tool improvements are tailored to address immediate cybersecurity concerns. These recommendations encompass strategic adjustments in risk management practices, governance frameworks, and collaborative initiatives. By integrating the case study's qualitative nuances with the tool's quantitative precision, these recommendations are poised to fortify the organization's cyber resilience swiftly.

To ensure the sustained effectiveness of the Cybersecurity Governance Tool, continuous improvement is imperative. Recommendations for enhancements align with the challenges identified in the case study and are informed by the evolving cybersecurity landscape. Regular updates to the tool, reflecting the latest standards and insights, will empower the organization to proactively adapt to emerging cyber threats. The integration of case study experiences into the tool's improvement strategy ensures a dynamic and responsive cybersecurity governance framework.

Conclusion: Coherence and Contribution The coherence achieved by synthesizing the case study and tool analysis underscores the importance of a balanced research approach. The qualitative depth provided by the case study harmonizes with the quantitative precision delivered by the Cybersecurity Governance Tool. This coherence ensures a robust and holistic understanding of the organization's cybersecurity governance landscape, reflecting a synergy between real-world experiences and analytical rigor.

The integration of case study insights and tool analysis has significantly contributed to the overarching objectives outlined in Chapter One. This holistic approach not only enriches academic discourse but also provides practical value for organizations navigating the complex realm of cybersecurity governance. The attached Cybersecurity Governance Tool in the Appendices serves as a tangible outcome of this research, offering a resource that organizations can leverage for comprehensive cybersecurity management.

Chapter 5

Results, Discussion, and Recommendations

5.1 Results, Discussion, And Recommendations

In this chapter, the results of rigorous research are revealed and discussed. The following sections intricately weave together the qualitative depth obtained from the case study with the quantitative precision derived from the Cybersecurity Governance Tool analysis. This integrated approach offers a panoramic view of the organization's cybersecurity governance landscape, aligning real-world scenarios with structured assessments.

5.1.1 The Study's Results

The study's results reveal significant insights into the impact of cybersecurity governance on mitigating cyber threats within organizations. Following the implementation of the Enterprise Governance of Information and Technology (EGIT) program and the integration of the COBIT 2019, NIST Cybersecurity Framework (CSF), and Sherwood Applied Business Security Architecture (SABSA) frameworks, the cybersecurity governance framework

emerged as a critical enabler in improving defenses against evolving cyber threats. The organization experienced a substantial improvement in its cybersecurity maturity, progressing from a CMMI maturity level of 1.3 to 2.7 within a year. This growth was driven by the structured and integrated approach to governance, which enhanced the visibility of the threat landscape and empowered the organization to identify, protect, detect, respond to, and recover from cybersecurity incidents in a more efficient and proactive manner.

The adoption of these frameworks led to significant improvements in the organization's incident response protocols. The dynamic capabilities of the cybersecurity governance tool, aligned with the COBIT 2019 and NIST CSF v1. 1, resulted in faster detection and reduced recovery times. Additionally, SABSA's architectural framework ensured that security controls were deeply embedded in the organization's infrastructure, providing stronger and more resilient systems. The table below demonstrates the improvements in the organization's incident response actions in 2023 compared to pre-implementation phases, under various attack classifications:

CSIRP Phase	Action	Pre-Implementation (2020-2021)	Post-Implementation (2023)
Malware			
Phase 1: Issue Identification	Detected via antivirus logs and suspicious file activity monitoring.	12/09/2020	14/05/2023
Phase 2: Investigation	IT team isolates affected systems for in-depth analysis.	12/11/2020	15/05/2023
Phase 3: Recovery	Systems cleaned, patches applied, and vulnerabilities addressed.	12/01/2021	16/05/2023
Phase 4: Reporting	Incident report submitted to senior management and NCA.	12/03/2021	18/05/2023
System Compromise			
Phase 1: Issue Identification	Alert received from intrusion detection system (IDS).	05/11/2020	22/06/2023

Phase 2: Investigation	Log analysis conducted to identify the compromised entry point.	05/01/2021	23/06/2023
Phase 3: Recovery	System restored from backup, vulnerabilities patched.	05/03/2021	24/06/2023
Phase 4: Reporting	Findings shared with stakeholders and regulatory authorities.	05/05/2021	26/06/2023
Denial of Service (DoS)			
Phase 1: Issue Identification	Network traffic analysis reveals high inbound traffic.	23/05/2021	03/04/2023
Phase 2: Investigation	The cybersecurity team investigates traffic origins and characteristics.	23/07/2021	04/04/2023
Phase 3: Recovery	Traffic filtered, network throttling applied, and attackers blocked.	23/09/2021	06/04/2023
Phase 4: Reporting	Report compiled for NCA and stakeholders.	23/11/2021	07/04/2023
Personal/ Sensitive Data Breach			
Phase 1: Issue Identification	Detected through abnormal data access logs.	15/03/2020	10/01/2023
Phase 2: Investigation	Data access and download logs reviewed to identify the breach scope.	15/05/2020	11/01/2023
Phase 3: Recovery	Access privileges revoked, affected systems reviewed for vulnerabilities.	15/07/2020	12/01/2023
Phase 4: Reporting	Breach reported to customers, regulatory authorities, and NCA.	15/09/2020	13/01/2023

Social Media Attacks			
Phase 1: Issue Identification	Alert from public relations team regarding unauthorized posts.	08/06/2020	15/02/2023
Phase 2: Investigation	Social media accounts reviewed, access logs checked.	08/08/2020	16/02/2023
Phase 3: Recovery	Unauthorized posts removed, credentials reset.	08/10/2020	17/02/2023
Phase 4: Reporting	Internal and external communications released.	08/12/2020	19/02/2023
Phishing Attacks			
Phase 1: Issue Identification	Multiple users report suspicious emails.	10/10/2020	18/08/2023
Phase 2: Investigation	The email headers and content are analyzed, sources blacklisted.	10/12/2020	19/08/2023
Phase 3: Recovery	Affected accounts are secured, employees receive training.	10/02/2021	20/08/2023
Phase 4: Reporting	Incident logged for senior management and stakeholders.	10/04/2021	21/08/2023
Insider Attacks			
Phase 1: Issue Identification	Unauthorized access patterns detected in the internal system.	21/08/2020	03/07/2023
Phase 2: Investigation	User activity logs reviewed, internal audit conducted.	21/10/2020	04/07/2023
Phase 3: Recovery	User privileges revoked, affected systems reviewed.	21/12/2020	05/07/2023

Phase 4: Reporting	Detailed report provided to legal and human resources departments.	21/02/2021	07/07/2023
Website Hacks			
Phase 1: Issue Identification	Web application firewall alerts unauthorized website access.	13/02/2021	28/09/2023
Phase 2: Investigation	Logs reviewed, vulnerabilities identified in the website backend.	13/04/2021	29/09/2023
Phase 3: Recovery	Vulnerabilities patched, website restored to a secure state.	13/06/2021	30/09/2023
Phase 4: Reporting	Incident reported to stakeholders and cybersecurity authority.	13/08/2021	02/10/2023

5.1.1.1 Analysis of Incident Response

The above table reflects the organization's improved cybersecurity maturity post-implementation of COBIT 2019, NIST CSF v1. 1, and SABSA. Pre-implementation, incident response processes were slower and often reactive. In 2023, after implementing these frameworks, the organization demonstrated quicker detection, investigation, and recovery times, resulting in improved resilience against cyber threats. The integration of proactive measures significantly reduced the impact of incidents, highlighting the value of a comprehensive governance approach in cybersecurity.

5.1.1.2 Quantitative Cybersecurity Risk Assessment and Analysis

A quantitative approach to cybersecurity risk assessment provides a more thorough and reliable understanding of the organization's risk posture. By leveraging metrics such as risk likelihood, impact, incident response times, and cost-benefit analysis, a comprehensive assessment of cybersecurity risks can be achieved. This section outlines key metrics used in the assessment of Organization Alpha.

5.1.1.3 Risk Metrics Overview

To evaluate cybersecurity risks quantitatively, the following key metrics were applied:

- **Risk Likelihood (L):** A measure of the probability of a given risk occurring, rated from 1 (Very Unlikely) to 5 (Very Likely).
- **Risk Impact (I):** A measure of the potential impact on the organization if the risk materializes, rated from 1 (Low Impact) to 5 (Severe Impact).
- **Inherent Risk (IR):** The risk level before any controls are applied, calculated as:

$$\text{Inherent Risk (IR)} = \text{Likelihood (L)} \times \text{Impact (I)}$$

- **Control Effectiveness (CE):** A percentage (0%-100%) that reflects how well the existing controls mitigate the identified risks.
- **Residual Risk (RR):** The remaining risk after controls are applied, calculated as:

$$\text{Residual Risk (RR)} = \text{Inherent Risk (IR)} \times \left(1 - \frac{\text{Control Effectiveness (CE)}}{100}\right)$$

- **Cost-Benefit Analysis:** The financial implications of mitigating risks vs. the potential cost of the risk materializing, helping to determine the effectiveness of control investments.
- **Incident Response Times:** The time it takes for the organization to detect, investigate, respond to, and recover from cybersecurity incidents, providing insight into the efficiency of the incident response procedures.
- **Number of Incidents Before and After Framework Implementation:** A measure of how the frequency of incidents has changed following the adoption of COBIT 2019, NIST CSF v1. 1, and SABSA frameworks.

5.1.1.4 Risk Assessment Matrix

The table below shows the risk matrix for Organization Alpha, highlighting the key risks, their likelihood, impact, inherent risk, control effectiveness, and residual risk. This quantitative strategy allows a more accurate evaluation of risks compared to a qualitative approach.

Risk Description	Likelihood (L)	Impact (I)	Inherent Risk (IR)	Control Effectiveness (CE)	Residual Risk (RR)
Lack of comprehensive Enterprise Architecture (EA)	3	4	12	50%	6
IT operational infrastructure incidents due to misconfigurations	5	5	25	60%	10
Unauthorized actions by insiders	4	5	20	70%	6
Hardware failures due to insufficient testing	4	4	16	40%	9.6
Software failure due to improper testing and configuration	3	4	12	50%	6
Cybersecurity attack resulting from vulnerabilities in network security	5	5	25	50%	12.5
Phishing attacks leading to data breaches	4	4	16	60%	6.4
Social media breaches causing unauthorized posts	3	3	9	80%	1.8
Denial of Service (DoS) attacks affecting availability	4	5	20	60%	8

5.1.1.5 Cost-Benefit Analysis

A cost-benefit analysis was conducted to assess the financial impact of cybersecurity risks in Organization Alpha. The analysis compared the cost of implementing controls to mitigate risks against the potential financial damage if the risks materialize without controls. For example, the mitigation of phishing attacks required an investment in employee training and email filtering solutions costing \$50,000, while the potential damage from phishing attacks could result in losses up to \$500,000, thus prevailing a significant return on investment.

- **Phishing Attack Mitigation Investment:** \$50,000
- **Potential Financial Loss from Phishing Attacks:** \$500,000
- **Benefit:** \$450,000 in avoided damages

This cost-benefit analysis underscores the importance of investing in cybersecurity measures, particularly for high-likelihood, high-impact risks such as network vulnerabilities and insider threats.

5.1.1.6 Incident Response Times

Before the implementation of COBIT 2019, NIST CSF v1. 1, and SABSA, Organization Alpha faced significant delays in its incident response times. The average time to detect and respond to incidents was between 72 hours and up to 50 days, leading to extended recovery periods and higher residual risk.

After the frameworks were implemented, the average incident response time was reduced to 72 hours or less, significantly improving the organization's ability to mitigate risks and recover from cyberattacks more efficiently.

- **Incident Response Time (Pre-Implementation):** 72 hours and up to 50 days
- **Incident Response Time (Post-Implementation):** 72 hours or less

5.1.1.7 Number of Incidents Before and After Framework Implementation

A key metric in assessing the effectiveness of the cybersecurity frameworks is the change in the number of incidents before and after the implementation of COBIT 2019, NIST CSF

v1. 1, and SABSA. Organization Alpha experienced a significant reduction in incidents after the frameworks were fully operational.

- **Number of Incidents (Pre-Implementation, 2020-2021):** 25 incidents
- **Number of Incidents (Post-Implementation, 2023):** 13 incidents

This reduction in the number of incidents demonstrates the effectiveness of the frameworks in reducing vulnerabilities and improving the overall security posture of the organization.

By incorporating quantitative metrics such as inherent and residual risks, cost-benefit analyses, incident response times, and incident frequency, the study provides a more comprehensive and reliable assessment of Organization Alpha's cybersecurity posture. This quantitative strategy clearly outperforms a purely qualitative approach, offering actionable insights into the risks faced by the organization and the effectiveness of the implemented cybersecurity controls.

5.1.1.8 Results of the Research Questions

In addressing the mechanism to deter cyber-attacks in a time-based approach, the organization emphasized a strong cybersecurity posture backed by a comprehensive set of controls derived from COBIT 2019, NIST CSF v1. 1, and SABSA. This encompassed preventive measures such as firewalls, secure configurations, and access controls before an attack. During an attack, effective cybersecurity monitoring played a pivotal role, enabling the prompt detection of anomalies. Post-attack, periodic cybersecurity drills, coupled with lessons learned, were conducted to enhance resilience. This integrated approach, guided by the proposed solutions, ensured a proactive and adaptive defense mechanism.

The proposed solutions demonstrated their effectiveness in minimizing the damage caused by various cyber-attacks. For instance, in the case of malware, the organization implemented a comprehensive Malware Protection Solution, covering prevention, detection, and response measures. This included antivirus software, intrusion prevention systems, firewalls, and sandboxing. Each solution was configured to perform real-time scans, conduct full system scans regularly, and respond to malware in a dedicated environment, showcasing a multi-layered defense strategy.

Similar meticulous approaches were adopted for other cyber-attacks. The organization's defenses were structured, documented in policies, standards, and procedures, and

supported by a RACI matrix, clearly defining roles and responsibilities. These efforts collectively contributed to reducing the impact of system compromise, denial of service, data breaches, social media attacks, phishing attacks, insider attacks, and website hacks. The study underscores the effectiveness of a well-integrated and comprehensive cybersecurity governance framework in addressing diverse cyber threats across different phases of an attack. The study's findings offer comprehensive answers to the research questions posed:

1. How does organizations' cybersecurity governance impact cyber threats?

The integration of the EGIT program and the adoption of NIST CSF v1. 1, COBIT 2019, and SABSA frameworks played a pivotal role in shaping the organization's cybersecurity governance. This dynamic approach significantly elevated the organization's ability to identify, assess, and mitigate cyber threats. The cybersecurity governance framework, supported by the governance tool, demonstrated a tangible impact on improving overall cybersecurity maturity levels. Enhanced visibility into the threat landscape empowered the organization to proactively address vulnerabilities and respond effectively to emerging cyber threats.

2. What is the mechanism to deter cyber-attacks in a time-based approach (before, during, and after)?

The organization implemented a robust time-based approach to deter cyber-attacks, incorporating elements from COBIT 2019, NIST CSF v1. 1, and SABSA. Before an attack, preventive measures, such as firewalls, secure configurations, and access controls, were deployed. During an attack, continuous monitoring of the cybersecurity landscape allowed for early detection of anomalies. Post-attack, the organization conducted periodic cybersecurity drills, incorporating lessons learned to enhance its resilience. This integrated strategy, guided by the proposed solutions, demonstrated the organization's commitment to proactive defense mechanisms throughout the cyber-attack lifecycle.

3. How can the proposed solutions reduce the damage caused by various cyber-attacks?

The proposed solutions, derived from the three integrated frameworks, showcased their effectiveness in minimizing the impact of diverse cyber-attacks. For malware, the organization implemented a comprehensive Malware Protection Solution, covering prevention, detection, and response measures. Similar meticulous approaches were adopted for system compromise, denial of service, data breaches, social media attacks, phishing attacks, insider attacks, and website hacks. The organization's proactive stance, documented controls, and structured defenses outlined in policies and procedures were instrumental in reducing the potential damage caused by cyber threats. This integrated and proactive cybersecurity

governance framework demonstrated a holistic and effective approach to addressing the multifaceted challenges posed by cyber threats.

The table presented encapsulates a comprehensive strategy for countering diverse cyber threats through a time-based approach. It delineates pre-attack preventive measures, during-attack monitoring and detection, and post-attack recovery processes. This integrated approach draws from the NIST CSF v1. 1, COBIT 2019, and SABSA frameworks and is guided by the cybersecurity governance tool.

article array longtable float

Comparison of NIST CSF v1. 1, COBIT 2019, and SABSA frameworks in the context of various cyber attack types.

Table 5.2: Comparison of NIST CSF v1. 1, COBIT 2019, and SABSA frameworks in the context of various cyber attack types.

Cyber Attack Type	NIST CSF v1. 1	COBIT 2019	SABSA
Malware			
Before:	Utilizes NIST guidelines for proactive measures like secure configurations.	Implements COBIT practices for preventive controls (firewalls, access controls).	Leverages SABSA for architectural design to segregate and contain malware impact.
During:	NIST emphasizes real-time monitoring and detection during malware events.	COBIT supports continuous monitoring to detect and respond to malware in early stages.	SABSA aids in monitoring the impact within the architectural context for swift response.
After:	NIST suggests post-event analysis and lessons learned for future prevention.	COBIT recommends post-event cybersecurity drills and analysis for improvement.	SABSA contributes to recovery measures and enhancing preventive mechanisms based on lessons learned.
System Compromise	NIST	COBIT	SABSA

Cyber Attack Type	NIST CSF v1. 1	COBIT 2019	SABSA
Before:	NIST guides in preventive measures like system hardening and secure configurations.	COBIT emphasizes risk management to address weaknesses in enterprise governance.	SABSA contributes to architectural impact, enhancing overall system security.
During:	NIST supports real-time monitoring and behavioral analysis during system compromise events.	COBIT ensures a time-based approach for efficient strategies before and during a compromise.	SABSA aids in monitoring the system's compromised state within the architectural context.
After:	NIST recommends post-event analysis and recovery strategies for system compromise incidents.	COBIT advocates periodic cybersecurity drills and learning from past incidents for resilience.	SABSA supports recovery measures, applying lessons learned to enhance overall system security.
Denial of Service	NIST CSF v1. 1	COBIT 2019	SABSA
Before:	NIST provides strategies for resilience and preventive controls before a DoS attack.	COBIT supports a time-based approach, ensuring efficient strategies before, during, and after a DoS attack.	SABSA aids in architectural design to prevent and mitigate DoS impacts.
During:	NIST emphasizes real-time monitoring and response strategies during a DoS attack.	COBIT ensures continuous monitoring during a DoS attack for effective detection and response.	SABSA contributes to architectural considerations for mitigating the impact during a DoS attack.
After:	NIST recommends post-event analysis and recovery measures for DoS incidents.	COBIT advocates periodic cybersecurity drills and analysis for learning and improvement after a DoS attack.	SABSA supports recovery measures, applying lessons learned to enhance overall system resilience after a DoS attack.

Cyber Attack Type	NIST CSF v1. 1	COBIT 2019	SABSA
Personal/ Sensitive Data Breach	NIST CSF v1. 1	COBIT 2019	SABSA
Before:	NIST promotes strong controls for data protection and encryption before a potential breach.	COBIT aligns IT objectives with enterprise goals, emphasizing data security as part of governance.	SABSA contributes to secure architectural design, minimizing the risk of personal data breaches.
During:	NIST emphasizes real-time monitoring and detection during a data breach event.	COBIT ensures a time-based approach for efficient strategies before and during a data breach.	SABSA aids in monitoring the breach impact within the architectural context for swift response.
After:	NIST suggests post-event analysis and recovery strategies for personal data breach incidents.	COBIT advocates periodic cybersecurity drills and learning from past incidents for resilience after a data breach.	SABSA supports recovery measures, applying lessons learned to enhance overall data security after a breach.
Social Media Attacks	NIST CSF v1. 1	COBIT 2019	SABSA
Before:	NIST encourages awareness and education on social engineering attacks as preventive measures.	COBIT supports governance practices that involve stakeholders and promote communication for social media security.	SABSA aids in architectural considerations to minimize the impact of social media attacks.
During:	NIST emphasizes real-time monitoring and response strategies during social media attacks.	COBIT ensures continuous monitoring during a social media attack for effective detection and response.	SABSA contributes to architectural considerations for mitigating the impact during a social media attack.

Cyber Attack Type	NIST CSF v1. 1	COBIT 2019	SABSA
After:	NIST recommends post-event analysis and recovery strategies for incidents involving social media attacks.	COBIT advocates periodic cybersecurity drills and analysis for learning and improvement after a social media attack.	SABSA supports recovery measures, applying lessons learned to enhance overall system resilience after a social media attack.
Phishing Attacks	NIST CSF v1. 1	COBIT 2019	SABSA
Before:	NIST emphasizes training and awareness to prevent falling victim to phishing attacks.	COBIT focuses on communication and involving stakeholders to address phishing challenges before they occur.	SABSA contributes to architectural defenses, reducing susceptibility to phishing attacks.
During:	NIST encourages real-time monitoring and response strategies during phishing attack events.	COBIT ensures continuous monitoring during a phishing attack for effective detection and response.	SABSA aids in monitoring the impact within the architectural context for swift response during a phishing attack.
After:	NIST recommends post-event analysis and recovery strategies for incidents involving phishing attacks.	COBIT advocates periodic cybersecurity drills and learning from past incidents for resilience after a phishing attack.	SABSA supports recovery measures, applying lessons learned to enhance overall system resilience after a phishing attack.
Insider Attacks	NIST CSF v1. 1	COBIT 2019	SABSA

Cyber Attack Type	NIST CSF v1. 1	COBIT 2019	SABSA
Before:	NIST highlights monitoring and behavioral analysis as preventive measures against insider threats.	COBIT enhances governance, ensuring a clear vision and communication to prevent insider attacks before they occur.	SABSA aids in architectural considerations for controlling and monitoring insider threats.
During:	NIST encourages real-time monitoring and response strategies during insider attack events.	COBIT ensures continuous monitoring during an insider attack for effective detection and response.	SABSA contributes to architectural considerations for mitigating the impact during an insider attack.
After:	NIST recommends post-event analysis and recovery strategies for incidents involving insider attacks.	COBIT advocates periodic cybersecurity drills and learning from past incidents for resilience after an insider attack.	SABSA supports recovery measures, applying lessons learned to enhance overall system resilience after an insider attack.
Website Hacks	NIST CSF v1. 1	COBIT 2019	SABSA
Before:	NIST suggests risk assessments, vulnerability scanning, and secure software development practices to prevent website hacks.	COBIT emphasizes the governance of IT, including maintaining secure configurations and regular patching to avoid vulnerabilities in website systems.	SABSA focuses on ensuring that the security architecture addresses potential vulnerabilities in the web environment, enforcing security policies.
During:	NIST emphasizes real-time monitoring, logging, and incident response processes during a website hack, as well as immediate containment.	COBIT ensures that incident response capabilities are activated and encourages quick decision-making and communication during the hack.	SABSA supports ongoing system monitoring and rapid response at the architectural level to mitigate the breach during the hack.

Cyber Attack Type	NIST CSF v1. 1	COBIT 2019	SABSA
After:	NIST advocates for post-incident analysis, implementing recovery protocols, and applying patches to prevent future attacks after a website hack.	COBIT promotes a structured review of the incident, ensuring that lessons learned are integrated into future governance and security protocols.	SABSA ensures that architectural updates are made post-attack, reinforcing the system against future hacks and improving resilience based on lessons learned.

In conclusion, the table demonstrates a cohesive and adaptable defense mechanism, emphasizing the importance of a holistic cybersecurity governance strategy in addressing the evolving landscape of cyber threats.

5.2 Discussion of Results

This study provides a unique contribution to the field of cybersecurity governance for critical infrastructure, particularly within the Saudi Arabian context. In Chapter 2, the literature review summarized existing research and theoretical perspectives, including widely used frameworks like COBIT 2019, NIST CSF v1.1, and SABSA, which underscore the importance of structured cybersecurity governance. However, the findings of this research reveal practical advancements and empirical insights that extend beyond these established frameworks, offering a distinct and actionable approach to enhancing cybersecurity resilience.

5.2.1 Contribution to Cybersecurity Governance Frameworks

The implementation of a tailored cybersecurity governance framework in this study demonstrated significant enhancements in organizational cybersecurity maturity and capability. Unlike the predominantly theoretical discussions in the literature, which often lack empirical data on practical outcomes, this study observed measurable improvements, with maturity levels increasing from 1.3 to 2.7 over a year. This empirical evidence highlights

the impact of a customized, adaptive approach to governance, suggesting that frameworks can achieve greater efficacy when adjusted to fit an organization's specific needs and contextual factors, especially within high-stakes environments such as critical infrastructure. This nuanced application of governance frameworks fills a gap in the literature, where customization and empirical validation have been limited.

5.2.2 Time-Based Cybersecurity Approach and Defense Strategies

Another notable contribution of this study is the exploration of a time-based cybersecurity strategy, integrating preventive, detective, and responsive controls at each stage of a cyber incident. Previous studies primarily emphasize layered defense strategies, but they often lack detailed models showing proactive measures before, during, and after attacks. The time-based approach presented in this study offers a more dynamic model for managing cybersecurity threats. By coordinating defense mechanisms throughout an attack's life-cycle, the organization demonstrated an enhanced ability to preempt, detect, and respond to cyber threats—a strategy not widely documented in existing literature but crucial for handling the complex, evolving threat landscape.

5.2.3 Effectiveness of Practical Solutions

The study also evaluated the practical effectiveness of specific cybersecurity solutions aligned with the implemented governance framework. Unlike previous research, which tends to discuss solutions in general terms, this study demonstrated the real-world applicability of these solutions in reducing the impact of cyberattacks, particularly against malware, system compromises, denial-of-service attacks, and data breaches. The multifaceted approach—employing tools such as intrusion prevention, regular scanning, and comprehensive monitoring—yielded tangible results, showcasing how a robust governance framework can address a range of cyber threats effectively. These findings contribute new perspectives to the literature, indicating that a governance framework's adaptability and versatility are critical to mitigating diverse cyber risks.

5.2.4 Implications for Cybersecurity in Critical Infrastructure

The findings underscore the importance of customizing cybersecurity governance models to address the unique requirements of critical infrastructure organizations. While much of the existing literature outlines generalized frameworks, the outcomes of this study underscore that organizations in high-risk environments may benefit from tailored frameworks that integrate established best practices with industry-specific needs. This study demonstrates the importance of adjusting governance approaches to account for the operational and contextual demands of critical infrastructure, a perspective less emphasized in existing research.

In conclusion, this study bridges the gap between theoretical cybersecurity governance models and their real-world application, providing practical insights into customizing, implementing, and measuring the effectiveness of a cybersecurity governance framework. It offers empirical evidence and a framework that can guide other critical infrastructure organizations aiming to enhance their cybersecurity resilience. This research thus contributes to the broader cybersecurity discourse by validating established theories and providing new, actionable insights tailored to critical infrastructure's unique cybersecurity challenges.

5.3 Contribution to the Field

This study makes significant contributions to the field of cybersecurity governance and resilience within critical infrastructure, particularly in the context of Saudi Arabia. The following key contributions highlight the insights and advancements brought forth by this research:

- **Integration of Dynamic Cybersecurity Governance Frameworks:** By integrating NIST CSF v1. 1, COBIT, SABSA, and CMMI V2.0 with cybersecurity governance tools, this research introduces a dynamic approach to cybersecurity governance assessment. This integration enables organizations to evaluate, enhance, and adapt established cybersecurity frameworks in real-time, fostering continuous improvement and resilience against evolving cyber threats.

- **Comprehensive Time-Based Cybersecurity Strategies:** The study's exploration of time-based cybersecurity strategies, encompassing preventive, detective, and deterrent controls before, during, and after cyber-attacks, provides a holistic defense mechanism. This

comprehensive approach not only enhances organizations' ability to mitigate cyber threats but also fosters proactive resilience, enabling swift adaptation to changing threat landscapes.

- **Efficacy Assessment of NIST Cybersecurity Framework Governed by COBIT 2019:** The evaluation of the National Institute of Standards and Technology (NIST) Cybersecurity Framework governed by Control Objectives for Information and Related Technologies (COBIT) 2019, in conjunction with the cybersecurity governance tool and CMMI V2.0, contributes empirical evidence on the effectiveness of these frameworks in minimizing the impact of cyber-attacks within critical infrastructure.

- **Architectural Impact Analysis of SABSA Framework:** This research investigate into the architectural impact of the Sherwood Applied Business Security Architecture (SABSA) framework, integrated with cybersecurity governance insights and CMMI V2.0 measures. The findings provide valuable insights into how SABSA contributes to the design of security capabilities, enhances cybersecurity governance, and effectively mitigates cyber threats.

- **Practical Adapted Frameworks' Capability Analysis:** Through a practical assessment of adapted cybersecurity frameworks, including NIST Cybersecurity Framework governed by COBIT 2019 and SABSA, this study offers insights into the capabilities of these frameworks in addressing diverse cyber threats. The analysis contributes to a nuanced understanding of cybersecurity governance's role in minimizing cyber risk within critical infrastructure.

- **Relationship Between Governance Practices and Cyber-Attacks:** By establishing a comprehensive understanding of the relationship between organizational cybersecurity governance practices and the occurrence, severity, and mitigation of cyber-attacks, this research bridges theoretical frameworks with practical outcomes. The insights gained provide a foundation for refining cybersecurity governance strategies to align with the unique challenges faced by critical infrastructure in Saudi Arabia.

In conclusion, this research extends the academic discourse on cybersecurity governance by introducing dynamic assessment frameworks, time-based strategies, and empirical evaluations of established cybersecurity frameworks. The contributions outlined above not only advance theoretical knowledge but also offer practical recommendations for enhancing cybersecurity resilience within critical infrastructure, contributing to the ongoing evolution of cybersecurity governance practices.

5.4 Study's Recommendations

Continuous Enhancement of Cybersecurity Governance: The success observed in the case study of Saudi Arabia's critical infrastructure highlights the vital importance of continually improving cybersecurity governance. In the context of Saudi Arabia's national strategy for securing critical assets, organizations shall adopt a proactive stance by regularly assessing and refining their cybersecurity governance frameworks. This iterative process should incorporate insights drawn from evolving cyber threats, global best practices, and advancements in technology, while considering the specific regulatory and operational environment in the Kingdom. This continuous improvement aligns with Saudi Arabia's Vision 2030 goals of building a robust and secure digital economy.

Adoption of Tailored Governance Tools: Saudi Arabian critical infrastructure organizations seeking to strengthen their defenses against cyber threats should prioritize the adoption of customized cybersecurity governance tools. In the case study, the practical application of such tools was instrumental in improving cybersecurity maturity. These tools should be tailored to the specific operational context of the organization and the national regulations within Saudi Arabia, ensuring they evolve to address both current and future cyber challenges. Customizing tools to the needs of the organization will help meet the unique demands of Saudi Arabia's critical sectors, such as oil, gas, finance, etc.

Integration of Time-Based Cybersecurity Strategies: The study emphasizes the effectiveness of adopting time-based cybersecurity strategies, especially within the framework of Saudi Arabia's critical infrastructure. It is recommended that organizations integrate preventive, detective, and deterrent controls across all stages of a cyber-attack—before, during, and after an incident. This comprehensive, layered defense ensures a dynamic approach that adapts to the increasingly sophisticated threat landscape targeting Saudi infrastructure. Regular cybersecurity drills and simulations, tailored to the specific risks faced by critical sectors in Saudi Arabia, should be conducted to evaluate and enhance the efficiency of these time-based strategies.

Optimized Implementation of COBIT 2019, NIST Cybersecurity Framework and SABSA: The research underscores the importance of optimizing the implementation of the National Institute of Standards and Technology (NIST) Cybersecurity Framework, in conjunction with the Control Objectives for Information and Related Technologies (COBIT) 2019 and Sherwood Applied Business Security Architecture (SABSA) frameworks. Saudi organizations should tailor these frameworks to their specific operational environments, taking into account regional threats and national cybersecurity guidelines. Leveraging these

frameworks, along with insights from the cybersecurity governance tools and Capability Maturity Model Integration V1.3 (CMMI), can ensure efficient adoption and a more robust cybersecurity posture.

Capacity Building and Skill Development: Addressing the shortage of cybersecurity skills and competencies is critical for Saudi Arabia's national security and economic stability. The case study highlighted this challenge, especially within critical infrastructure organizations. To overcome this, there shall be a significant investment in capacity building, including training programs focused on governance, cybersecurity management, and technical skills. Development initiatives such as coaching, mentoring, and cross-skilling are vital to empowering personnel to effectively implement and adapt cybersecurity governance measures, especially as Saudi Arabia continues to scale its digital transformation efforts under Vision 2030.

Periodic Cybersecurity Maturity Assessments: To ensure the sustained efficacy of cybersecurity governance measures within Saudi Arabia's critical infrastructure, periodic cybersecurity maturity assessments are essential. These assessments, following the methodology outlined in the study, provide valuable insights into the organization's readiness to combat emerging cyber threats. Organizations should benchmark their practices against both national and international standards, collaborating with external auditors and regulatory bodies within the Kingdom to strengthen their cybersecurity posture. Such assessments align with the broader goals of national security and resilience as set by the Saudi National Cybersecurity Authority (NCA).

Global Collaboration and Information Sharing: Cyber threats know no borders, and Saudi Arabia's critical infrastructure is not immune to global cyber adversaries. Therefore, organizations within the Kingdom are encouraged to actively participate in global forums, share threat intelligence, and collaborate on cybersecurity initiatives both regionally and internationally. This collective approach enhances Saudi Arabia's resilience against sophisticated cyber threats while aligning with global cybersecurity practices and regulations. By strengthening ties with international allies and contributing to global information-sharing networks, Saudi Arabia can bolster its critical infrastructure protection.

Conclusion: These recommendations provide a clear roadmap for Saudi Arabian critical infrastructure organizations aiming to enhance their cybersecurity governance and resilience against cyber threats. The dynamic nature of cyber threats demands an ongoing, adaptive approach, where organizations actively engage with emerging technologies, best practices, and Saudi Arabia's evolving regulatory environment to safeguard the Kingdom's

critical infrastructure in an increasingly digital landscape.

5.5 Limitations of the Study and Future Considerations

In this section, the research explores the limitations encountered during this study, shedding light on areas that require further investigation and focus. Understanding these limitations is essential for interpreting the study's findings accurately and identifying opportunities for future research and development.

5.5.1 Limitations of the Study

While this research endeavors to contribute valuable insights into the realm of cybersecurity governance, it is crucial to acknowledge certain limitations that may impact the scope and generalizability of the findings:

- **Geographical Context:**

- o **Limitation:** The study primarily focuses on the cybersecurity governance landscape within the critical infrastructure of Saudi Arabia. Consequently, the findings may have limited generalizability to other geographical contexts with distinct regulatory environments and cybersecurity challenges.

- **Industry Specificity:**

- o **Limitation:** The research centers on critical infrastructure sectors, potentially limiting the applicability of the proposed cybersecurity governance framework to other industries. Different sectors may have unique cybersecurity requirements that this study does not explicitly address.

- **Case Study Nature:**

- o **Limitation:** The research heavily relies on a comprehensive case study within a specific critical infrastructure setting in Saudi Arabia. While this approach provides in-depth insights, it may not capture the diversity of cybersecurity governance practices across various organizations.

- **Temporal Dynamics:**

- o **Limitation:** The dynamic nature of cybersecurity poses challenges in capturing real-time changes. The study's findings may be subject to temporal constraints, and the pro-

posed cybersecurity governance framework may require periodic reassessment to remain effective.

- External Factors:

- o Limitation: The efficacy of the proposed framework may be influenced by external factors such as evolving cyber threats, technological advancements, or changes in the regulatory landscape. The study acknowledges these external variables but may not comprehensively account for unforeseen developments.

- Tool-Specific Limitations:

- o Limitation: The cybersecurity governance tool developed for this research, while comprehensive, may have limitations in adapting to diverse organizational structures and sizes. Its effectiveness could be influenced by organizational nuances that are not fully captured.

- CMMI V2.0 Model Constraints:

- o Limitation: While the study integrates the Capability Maturity Model Integration V1.3 (CMMI) for assessing maturity and capability, the model itself has inherent limitations. Variability in interpretation and application across organizations may affect the consistency of assessments.

- Single-Case Study:

- o Limitation: The focus on a single critical infrastructure case study may limit the generalizability of the findings. Replicating the study across multiple critical infrastructures could provide a more comprehensive understanding.

Acknowledging these limitations is essential for maintaining transparency and ensuring that the study's outcomes are interpreted within the defined boundaries. Future research endeavors may address these limitations to refine and expand the proposed cybersecurity governance framework.

5.5.2 Future Considerations

The success of the cybersecurity governance framework and tool in the case study prompts considerations for future research and practical implementations. Comparative studies across different critical infrastructure sectors and regions could offer broader insights. Moreover, ongoing advancements in cyber threats necessitate continuous refinement of governance frameworks, emphasizing the need for adaptive and scalable solutions.

In conclusion, the discussion highlights the transformative impact of a tailored cy-

bersecurity governance framework and tool, emphasizing practical enhancements in the organization's cybersecurity maturity and capability. The study contributes not only to theoretical knowledge but also offers pragmatic insights for organizations navigating the intricate landscape of cybersecurity governance. Future endeavors should focus on refining and expanding these insights to foster a resilient and adaptive cybersecurity environment globally.

5.6 Conclusion

In conclusion, this thesis embarked on a comprehensive exploration of cybersecurity governance within the context of safeguarding critical national infrastructure. The urgency of addressing the escalating cyber threats to national infrastructure, coupled with the considerable economic losses associated with security breaches, underscored the need for a nuanced and dynamic approach.

The research objectives were meticulously designed to unravel the intricate facets of organizational practices impacting cyber threat resilience. By incorporating a cybersecurity governance tool and leveraging the Capability Maturity Model Integration V1.3 (CMMI), this study researched the impact of time-based cybersecurity strategies, the efficacy of renowned frameworks like the NIST Cybersecurity Framework governed by COBIT 2019, and the architectural impact of SABSA framework.

The research outcomes, as illuminated by the case study, provide a compelling narrative of the tangible enhancements achieved in the cybersecurity maturity and capability of the studied organization. The organization's journey, marked by the implementation of the Cybersecurity Governance framework and EGIT program, showcased a remarkable improvement in visibility, risk identification, protection, detection, response, and recovery capabilities. Notably, the maturity levels escalated from 1.3 to 2.7 within a year, validating the efficacy of the adopted measures. The recommendations put forth emphasize the importance of continuous enhancement, adoption of tailored governance tools, integration of time-based cybersecurity strategies, optimized implementation of frameworks, capacity building, periodic assessments, and global collaboration. These recommendations serve as a practical roadmap for organizations navigating the complex landscape of cybersecurity governance, providing insights to fortify critical infrastructure against evolving cyber threats.

As the cyber world navigates an era of relentless digitization and evolving cyber threats,

the findings and recommendations of this thesis contribute not only theoretical insights but also practical strategies for organizations aiming to bolster their cybersecurity postures. The dynamic nature of cyber threats necessitates a proactive and adaptive approach, and this research seeks to empower organizations in their quest for resilient and robust cybersecurity governance.

ملخص الدراسة

إنَّ تزايد وتيرة وتطور التهديدات السيبرانية، وخاصة تلك التي تستهدف البنية التحتية الوطنية الحيوية، يؤكد الحاجة الملحة لإطار حوكمة فعال في مجال الأمن السيبراني. تتناول هذه الدراسة فجوة كبيرة في فهم وتطبيق حوكمة الأمن السيبراني المصممة خصيصًا للبنية التحتية الحيوية في المملكة العربية السعودية، وهي قطاع يواجه ضعفًا متزايدًا أمام المخاطر السيبرانية المعقدة. باستخدام منهجية دراسة حالة شاملة، تقوم هذه الدراسة بدمج نموذج نضج التكامل (CMMI V1.3) مع أطر رائدة أخرى - مثل NIST CSF v1.1، و COBIT 2019، و SABSA. يوفر جمع البيانات من عام 2022 إلى 2024 تقييمًا شاملاً لنضج وقدرة ومرونة حوكمة الأمن السيبراني داخل منظمة للبنية التحتية الحيوية.

من خلال برنامج EGIT (حوكمة تقنية المعلومات على مستوى المؤسسة) المكون من خمس مراحل متسلسلة، تقوم هذه المنهجية بتقييم وتعزيز حوكمة الأمن السيبراني بشكل دقيق. تقنيات القياس في CMMI V1.3 تساعد في تقييم مستويات النضج عبر ضوابط الأمن السيبراني، مما يُمكن كل وحدة عمل من إجراء تقييمات ذاتية وتعديل الأهداف بناءً على القدرات ومستوى النضج. ومن خلال دمج استراتيجيات زمنية وأدوات حوكمة مخصصة، تُظهر الدراسة تقدمًا ملحوظًا في النضج من المستوى 1.3 إلى 2.7 خلال عام واحد، مما يعكس تحسنًا كبيرًا في مرونة المنظمة.

تكشف النتائج الرئيسية عن الأثر العملي لحوكمة الأمن السيبراني في حماية البنية التحتية الحيوية، والتي تم تحقيقها من خلال تنفيذ أطر حوكمة تم تكييفها خصيصًا للسياق السعودي. تبرز الدراسة مقارنة فريدة من نوعها تجمع بين أطر COBIT و NIST CSF و SABSA ضمن إطار متماسك يتماشى مع الأنظمة الوطنية - مما يقدم رؤى جديدة حول فوائد دمج نماذج الحوكمة المتعارف عليها مع الاحتياجات الخاصة بالمنطقة. إنَّ نموذج التحسين المستمر المقترح، الذي يشمل تقييمات نضج CMMI وتقييمات دورية للتهديدات، يعزز المرونة المستدامة مع تطور مشهد التهديدات. لا تعزز هذه الدراسة الإطار النظري لحوكمة الأمن السيبراني فحسب، بل تقدم أيضًا توصيات عملية لمنظمات البنية التحتية الحيوية في المملكة العربية السعودية، بما يتماشى مع أهداف رؤية المملكة 2030 لبناء اقتصاد رقمي قوي وآمن.

جامعة البحرين

كلية تقنية المعلومات

قسم هندسة الكمبيوتر



إطار حوكمة الأمن السيبراني للتخفيف
من الهجمات السيبرانية:
دراسة حالة في المملكة العربية السعودية
أطروحة مقدمة كجزء من متطلبات الحصول على
درجة ماجستير العلوم في الأمن السيبراني

إعداد

أروى الرميح

٢٠١٩٠٢٦٦

إشراف

د. مازن علي

(أستاذ مشارك)

جامعة البحرين

مملكة البحرين

٢٠٢٤ نوفمبر

Appendix

Interview Logs:

Assessment Questionnaire

1. Demographic Characteristics:

1. Age of Assessment Participants:

The age majority 35-55; 1 under 35.

2. Educational Attainment:

Mainly bachelor's degree except for 1 with master's degree working under the IT. The majority have IT professional certificates. However, a few to none related to cybersecurity.

3. Work Experience:

Mainly they are from 5 years to 25 years.

4. Roles and Responsibilities:

I meet the following personnel: vice president, CIO, Cybersecurity manager, SME from GRC, SME from Access management, SME from IT, SME from IT project management.

2. Initial Assessment Responses:

1. How is the IT/Cybersecurity department structured?

The organization's subject matter expert (SME) response: The cybersecurity department reports to Information Technology under the Chief Information Officer (CIO).

2. What's the current IT/Cybersecurity model? On-premises? Outsourced or hybrid?

The organization's SME response: The current IT/Cybersecurity model is hybrid. Some of the services are on-premises, while others are outsourced.

3. How many IT/Cybersecurity staff do you have?

The organization's SME response: The total number of IT/Cybersecurity staff is 30 employees. 22 are IT while 8 employees working in the Cybersecurity department. Male 22, and female 8.

4. Do you apply IT/Cybersecurity Governance? How?

The organization's SME response: Yes. Cybersecurity Governance applied based on the Saudi National Cybersecurity Authority (NCA) cybersecurity Essential Cybersecurity Controls, and ISO 27001.

5. How is the cybersecurity department structured? If not, does the function exist? Or outsourced?

The organization's SME response: Cybersecurity is reporting to the CIO. The cybersecurity department mainly covers Risk, Governance, Compliance (GRC), and Access management. On the other hand, cybersecurity operations are currently outsourced to a cybersecurity manager services provider in Saudi Arabia; but it is governed by the GRC team.

6. Is your company subject to international or local regulatory requirements such as Saudi Cybersecurity Authority (NCA), Capital Market Authority, or Saudi Authority for Data and Artificial Intelligence (SADIA)? If so, how was your compliance result? If not, are you considering it in the future?

The organization's SME response: The company is subject to the NCA regulation in addition to the Saudi Authority for Data and Artificial Intelligence (SADIA). For international requirements, it is not. However, it is highly recommended because the company is currently in the process of becoming a publicly traded company. Therefore, it will be subject to the Saudi Capital Market Authority cybersecurity regulations, which some of which are based on NIST in addition to their guidelines "Secure by Design."

7. Who is responsible for cybersecurity in your organization?

The organization's SME response: Cybersecurity is everyone's responsibility. However, formal responsibility is scattered between IT, the cybersecurity team, and the managed cybersecurity service provider.

8. Do you have a chief information security officer (CISO)?

The organization's SME response: Currently, there is no CISO. There is only a Cybersecurity manager. However, we are interviewing multiple candidates

to hire a CISO. This is one of the requirements of the Saudi Capital Market Authority before becoming a publicly traded company in alignment with their Cybersecurity Guidance for Capital Marker Institutions.

9. Do you regularly meet, across company departments, to discuss and monitor cybersecurity issues?

The organization's SME response: Cybersecurity issues are raised during the weekly management communication meetings. However, it is not conducted for cybersecurity only.

10. How do you protect customer information? Please be specific.

The organization's SME response: Customer information is being protected through ensuring adherence to the required cybersecurity requirements mandated by NCA and SDAIA, ISO, etc.

11. Have you ever experienced a significant cybersecurity incident? Please define and describe the incident.

The organization's SME response: Yes, unfortunately, we had a few significant cybersecurity incidents. We had cases with successful phishing attacks, which helped lead to another spear phishing attack. We had a ransomware attack. We also had an insider incident.

12. How are cybersecurity incidents reported?

The organization's SME response: Incident is reported either by the cybersecurity managed service provider, GRC team, or by the IT personnel. Once it's confirmed, executive management is briefed about it. Also, local law authorities might get involved.

13. When was the last time you had a cybersecurity assessment performed by a third-party organization? What were the results?

The organization's SME response: Last independent 3rd party cybersecurity assessment was conducted 3 years ago. We conduct our cybersecurity assessment annually by the GRC team. The result varies depending on changes in the environment. The outcome of the assessment will show gaps and it ended up with an action plan to be monitored by the management.

14. What were the results of your most recent vulnerability assessment or penetration test?

The organization's SME response: For the vulnerability assessments, several

vulnerabilities are being fixed within a specific timeline and based on their severity in alignment with the required company's cybersecurity standards.

15. Do you outsource any IT or cybersecurity functions to third-party service providers? If so, who are they, what do they do, and what type of access do they have?

The organization's SME response: Yes, just like any other organization, there are a number of functions and processes that are outsourced to a 3rd party. For example, for the IT Department IT field support, help desk, application development is outsourced. For the cybersecurity department, security monitoring center, endpoint security, vulnerability assessment, network security, email security is outsourced to a local cybersecurity managed service provider. In terms of access, they have access to the needed services with administrative access privileges to perform their needed tasks.

Conducted Workshops Details:

Table 5.3: Conducted Workshops Details

Workshop Topic	Workshop Date	Status
Get to know the organization (Background, Business Challenges, etc.)	Aug 11, 2022	Completed
Get to know the organization (Background, Business Challenges, etc.)	Aug 11, 2022	Completed
Conduct the initial assessment; the assessment questions in part 7. Appendices.	Sep 8, 2022	Completed
Introduction to COBIT 2019, NIST CSF v1. 1, and SABSA frameworks	Sep 18, 2022	Completed
Explain the overall key benefits of this methodology and the assessment process	Sep 18, 2022	Completed
Identify the objectives, primary and secondary strategy, and enterprise goals	Sep 18, 2022	Completed
View the organization's risk profile, I and T-related issues, threat landscape, compliance requirements, role of IT, sourcing model for IT, IT implementation methods, technology adoption strategy, enterprise size, etc.	Oct 13, 2022	Completed
Evaluate the Performance Management of Organizational Structures and Performance Management of Culture and Behavior	Oct 13, 2022	Completed
Identify the stakeholders and business needs	Oct 13, 2022	Completed
Aligning business needs and goals with the frameworks	Oct 13, 2022	Completed
EGIT program five delivery sequential phases	Oct 23, 2022	Completed
Analysis the provided documents	Oct 23, 2022	Completed
Evaluate current security practices, controls, processes, etc.	Oct 23, 2022	Completed
Assess current (as-is) cybersecurity capability utilizing CMMI V2.0	Oct 23, 2022	Completed

Define target state and recommendations	Oct 23, 2022	Completed
Design the EGIT framework part (1)	Nov 6, 2022	Completed
Design the EGIT framework adding the NIST CSF v1. 1 part (2)	Nov 6, 2022	Completed
Design the EGIT framework adding the NIST CSF v1. 1 and including SABSA part (3)	Nov 6, 2022	Completed
Present the implementation of the 3 frameworks in the organization	Dec 22, 2022	Completed
Present the best practices for integrating the frameworks	Dec 22, 2022	Completed
Evaluate the implementation	Dec 22, 2022	Completed
Present monitoring and enhancement best practices	Dec 22, 2022	Completed
Follow-up visit to reevaluate the cybersecurity capability utilizing CMMI V2.0	Jun 15, 2023	Completed
Reevaluate the implementation	Jun 15, 2023	Completed
Assess the compliance percentage based on the NCA ECC	Jun 15, 2023	Completed
Verify the proposed solutions of integrated 3 frameworks	Sep 14, 2023	Completed

List of Observed IT Infrastructure Assets, New Systems, and Documents

Policies

1. General Cyber Security Policy
2. Compliance Policy With Cyber Security Legislation And Regulations
3. Settings And Immunization Policy
4. Malware Protection Policy

5. Server Security Policy
6. Network Security Policy
7. Security Policy For Users' Devices, Mobile Devices, And Personal Devices
8. Asset Acceptable Use Policy
9. Managing Update And Fix Packages Policy
10. Third-Party Cyber Security Policy
11. Vulnerability Management Policy
12. Cybersecurity Incidents and Threats Management Policy
13. Information Protection Policy

Standards

1. Network Security Standard
2. Email Security Standard
3. User Device Security Standard
4. Mobile Device Security Standard
5. Server Security Standard
6. Database Security Standard
7. Vulnerability Management Standard
8. Wireless Network Security Standard

Procedure and Process

1. Risk Management Framework
2. Compliance Management Framework
3. Roles and Responsibilities
4. Organizational Structure
5. IT Strategy
6. Business Strategy
7. Backup and Restore Architecture
8. Architecture of Identity Access Management
9. Privileged Access Management (PAM) Architecture Design
10. Enterprise Multifactor Authentication
11. SAP SuccessFactors Architecture Design
12. IT Asset Inventory
13. SOC Processes
14. Cybersecurity Incidents Last 30 Days

Security Baseline

1. Microsoft Windows 11 Enterprise
2. Microsoft Windows Server 2012
3. Microsoft Windows Server 2019
4. Apache HTTP Server
5. Red Hat Enterprise Linux 9

6. Cisco IOS
7. Fortinet Web Application Firewalls
8. Palo Alto Firewall
9. VMware ESXi
10. Oracle Database
11. FireEye
12. Cisco IOS SSL VPN
13. Cisco Router/Switch

Malware Protection

1. McAfee
2. Microsoft Defender

PUBLICATIONS

This thesis is based on previously published papers written jointly with Dr. Yasser Ismail, and Dr. Wael Elmedany:

JOURNAL PAPERS

(Published) Arwa Alromaih, Dr. Yasser Ismail, and Dr. Wael Elmedany. "Continuous Compliance to Ensure Strong Cybersecurity Posture Within Digital Transformation In Smart Cities" 6th Smart Cities Symposium (SCS 2022). IEEE Xplore: 29 May 2023. URL: <https://ieeexplore.ieee.org/document/10137541>

CONFERENCE PAPERS

(Published) Arwa Alromaih, Dr. Yasser Ismail, and Dr. Wael Elmedany. "Continuous compliance to ensure strong cybersecurity posture within digital transformation in smart cities" In 6th Smart Cities Symposium (SCS 2022), 2022 p. 464 – 479. URL: <https://digital-library.theiet.org/content/conferences/10.1049/icp.2023.0647>

References

- Alashi, S. A., & Badi, D. H. (2020). The role of governance in achieving sustainable cybersecurity for business corporations. *Journal of Information Security and Cybercrimes Research*, 3(1), 97–112.
- AlDaajeh, S., & Alrabae, S. (2024). Strategic cybersecurity. *Computers & Security*, 141, 103845.
- AlGhamdi, A. A., Niazi, M., Alshayeb, M., & Mahmood, S. (2024). Organizations' readiness for insider attacks: A process-oriented approach. *Software: Practice and Experience*.
- Alhejaili, M. O. M. (2024). Securing the kingdom's e-commerce frontier: Evaluation of saudi arabia's cybersecurity legal frameworks. *Journal of Governance and Regulation/Volume*, 13(2).
- Ali, M. M., & Mohd Zaharon, N. F. (2024). Phishing—a cyber fraud: The types, implications and governance. *International Journal of Educational Reform*, 33(1), 101–121.
- Aljeaid, Alzhrani, Alrougi, & Almalki. (2020). Assessment of end-user susceptibility to cybersecurity threats in saudi arabia by simulating phishing attacks. *Information*, 11(12), 547. doi: 10.3390/info11120547
- Al-Mudaires, F., Al-Samawi, A., Aljughaiman, A., & Nissirat, L. (2023). Information security risk management framework for

- a governmental educational institute. *Journal of Information and Knowledge Management (JIKM)*, 13(1), 36–54.
- Al-Mulhim, R. A., Al-Zamil, L. A., & Al-Dossary, F. M. (2020). Cyber-attacks on saudi arabia environment. *International Journal of Computer Networks and Communications Security*, 8(3), 26–31.
- Alotibi, G. (2024). A cybersecurity awareness model for the protection of saudi students from social media attacks. *Engineering, Technology & Applied Science Research*, 14(2), 13787–13795.
- Alromaih, A., Abdulwahab, A., & Zeki, A. (2021). The impact of covid-19 pandemic on the rise of cyber security risks with an islamic view. *International Journal on Islamic Applications in Computer Science and Technology*, 9(3).
- Alzaabi, F. R., & Mehmood, A. (2024). A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods. *IEEE Access*, 12, 30907–30927.
- Andorno, P. (2024). *Research, testing, and mitigation solutions for web application firewalls evasion techniques* (Unpublished doctoral dissertation). Politecnico di Torino.
- Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, 12(6), 1333.
- Awan, T. M., & Pitafi, Z. R. (2024). Perspective chapter: Cybersecurity and risk management—new frontiers in corporate governance.
- Bandari, V. (2023a). Enterprise data security measures: a comparative review of effectiveness and risks across different industries and organization types. *International Journal of Business Intel-*

ligence and Big Data Analytics, 6(1), 1–11.

Bandari, V. (2023b). Enterprise data security measures: a comparative review of effectiveness and risks across different industries and organization types. *International Journal of Business Intelligence and Big Data Analytics*, 6(1), 1–11.

Cantelmi, R., Di Gravio, G., & Patriarca, R. (2021). Reviewing qualitative research approaches in the context of critical infrastructure resilience. *Environment Systems and Decisions*, 41(3), 341–376.

CMMI Version 2.0. (2018).

COBIT 2019 Framework. (2018). <https://www.isaca.org/cobit/pages/default.aspx>.

Cyberlands.io Team. (2023). *Top 9 cybersecurity breaches in saudi arabia*. Retrieved from <https://www.cyberlands.io/topsecuritybreachessaudiarabia> (Accessed: 2023-08-26)

Darmi, Y., Fernandez, S., Fathoni, M. Y., & Wijayanto, S. (2024). Evaluation of governance in information systems security to minimize information technology risks. *INTENSIF: Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi*, 8(1), 40–51.

Degerli, M. (2020). Practical suggestions to successfully adopt the cmmi v2. 0 development for better process, performance, and products. In *2020 5th international conference on computer science and engineering (ubmk)* (pp. 126–129).

Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. *Journal of Management Analytics*, 7(2), 189–208.

Doe, Jane, White, & Alan. (2021). Solarwinds cyberattack: Un-

- covering the implications of a global supply chain compromise. *International Journal of Cyber Threat Analysis*, 9(1), 45–60.
- Farayola, O. A., Olorunfemi, O. L., & Shoetan, P. O. (2024). Data privacy and security in it: a review of techniques and challenges. *Computer Science & IT Research Journal*, 5(3), 606–615.
- Fevid, E., Walsh, C., & Russo, L. (2024). Zero-day ransomware detection via assembly language bytecode analysis and random forest classification. *Authorea Preprints*.
- George, A. S., Baskar, T., & Srikanth, P. B. (2024). Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. *Partners Universal International Innovation Journal*, 2(1), 51–75.
- Georgiadou, A., Mouzakitou, S., & Askounis, D. (2021). Assessing mitre attack risk using a cyber-security culture framework. *Sensors*, 21(9), 3267.
- Greiman, V. (2023). Known unknowns: the inevitability of cyber attacks. In *European conference on cyber warfare and security* (Vol. 22, pp. 223–231).
- Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, 58, 102726.
- Hawdon, J. (2021a). Cybercrime: Victimization, perpetration, and techniques. *American Journal of Criminal Justice*, 46(6), 837–842.
- Hawdon, J. (2021b). Cybercrime: Victimization, perpetration, and techniques. *American Journal of Criminal Justice*, 46(6), 837–842.
- Institute, C. (2021). *Cmmi v2.0: A model for improving organi-*

zational performance. <https://cmmiinstitute.com/cmmi>.
(Available at: <https://cmmiinstitute.com/cmmi>)

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC). (2013). *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements* (Tech. Rep.).

Kelley, D., & Moyle, E. (2023). *Practical cybersecurity architecture: A guide to creating and implementing robust designs for cybersecurity architects*. Packt Publishing Ltd.

Kerner, S. M. (2022). *34 cybersecurity statistics to lose sleep over in 2022* (Tech. Rep.).

Kumari, P., & Jain, A. K. (2023). A comprehensive study of ddos attacks over iot network and their countermeasures. *Computers & Security*, 127, 103096.

Lee, H.-W. (2024). Malware attack indicators of compromise generation and sharing mechanism for cyber threat intelligence. In *Proceedings of the 2024 13th international conference on software and computer applications* (pp. 90–96).

Leszczyna, R. (2021). Review of cybersecurity assessment methods: Applicability perspective. *Computers & Security*, 108, 102376.

Melaku, H. M. (2023). A dynamic and adaptive cybersecurity governance framework. *Journal of Cybersecurity and Privacy*, 3(3), 327–350.

Möller, D. P. (2023). Nist cybersecurity framework and mitre cybersecurity criteria. In *Guide to cybersecurity in digital transformation: Trends, methods, technologies, applications and best practices* (pp. 231–271). Springer.

Muthuswamy, V. V. (2023). Cyber security challenges faced by em-

- ployees in the digital workplace of saudi arabia's digital nature organization. *International Journal of Cyber Criminology*, 17(1), 40–53.
- Najafimehr, M., Zarifzadeh, S., & Mostafavi, S. (2023). Ddos attacks and machine-learning-based detection methods: A survey and taxonomy. *Engineering Reports*, 5(12), e12697.
- National Cybersecurity Authority. (2018). *Essential cybersecurity controls*. Retrieved from <https://nca.gov.sa/en/regulatory-documents/controls-list/191/> (Retrieved September 18, 2024)
- (NCA), N. C. A. (2021). Organizational social media accounts cybersecurity controls framework (osmacc -1:2021). *National Cybersecurity Authority*. Retrieved from <https://nca.gov.sa/ar/osmacc-en.pdf>
- of Standards, N. I., & Technology. (2018). *Framework for improving critical infrastructure cybersecurity, version 1.1*. <https://www.nist.gov/cyberframework>. (Available at: <https://www.nist.gov/cyberframework>)
- Pascoe, C. E. (2023). Public draft: The nist cybersecurity framework 2.0.
- Petkova, L. (2020). Cms security tips and tricks. *Security & Future*, 4(2), 61–63.
- Potter, K., & Stilinski, D. (2024). *The economic impact of cybersecurity threats on businesses in developing economies: A cost-benefit analysis of it security investments* (Tech. Rep.).
- Sadqi, Y., & Maleh, Y. (2022). A systematic review and taxonomy of web applications threats. *Information Security Journal: A Global Perspective*, 31(1), 1–27.
- Saha, B., & Anwar, Z. (2024). A review of cybersecurity challenges in

- small business: The imperative for a future governance framework. *Journal of Information Security*, 15(01), 24–39.
- Sahoo, S., & Bharathi, S. V. (2023). Threats and countermeasures in online social networks: A systematic review of existing research and future directions. In *Aip conference proceedings* (Vol. 2869).
- Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. *International Cybersecurity Law Review*, 3(1), 7–34.
- Securing the Grid*. (2020). <https://nca.gov.sa/en/reports?item=216>.
- Setiadi, L. H., & Fianty, M. I. (2024). Enhancing organizational performance through cobit 2019-based it governance audit: A case study of a digital technology company. *Journal of Information Systems and Informatics*, 6(2), 676–688.
- Shah, A., Varshney, S., & Mehrotra, M. (2024). Threats on online social network platforms: classification, detection, and prevention techniques. *Multimedia Tools and Applications*, 1–33.
- Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., & Xu, M. (2020). A survey on machine learning techniques for cyber security in the last decade. *IEEE access*, 8, 222310–222354.
- Sherwood, Clark, & Lynas. (2005). *Enterprise security architecture: A business-driven approach*. SABSA Institute.
- Simons, G., Danyk, Y., & Maliarchuk, T. (2020). Hybrid war and cyber-attacks: creating legal and operational dilemmas. *Global Change, Peace & Security*, 32(3), 337–342.
- Smith, A., John, Jones, T., & Emily. (2018). The equifax data breach: Analyzing the largest personal data breach in history. *Journal of Cybersecurity*, 12(4), 23–37.

- Snow, S. (2020). A qualitative study of strategy-driven, information security governance (isg).
- Software Engineering Institute. (2022, September 7). *Common sense guide to mitigating insider threats, seventh edition* (Tech. Rep.). Retrieved from <https://insights.sei.cmu.edu/library/common-sense-guide-to-mitigating-insider-threats-seventh-edition/> (Retrieved September 18, 2024)
- Thakur, M. (2024). Cyber security threats and countermeasures in digital age. *Journal of Applied Science and Education (JASE)*, 4(1), 1–20.
- Valavanis, S. (2024). Understanding cybersecurity maturity in practice. *Journal of Information Systems*, 1–5.
- Wang, B., He, Y., Shui, Z., Xin, Q., & Lei, H. (2024). Predictive optimization of ddos attack mitigation in distributed systems using machine learning. *Applied and Computational Engineering*, 64, 95–100.
- Wosah, P. N., Ali Mirza, Q., & Sayers, W. (2024). Analysing the email data using stylometric method and deep learning to mitigate phishing attack. *International Journal of Information Technology*, 1–14.
- Zekri, M., El Kafhali, S., Aboutabit, N., & Saadi, Y. (2017). Ddos attack detection using machine learning techniques in cloud computing environments. In *2017 3rd international conference of cloud computing technologies and applications (cloudtech)* (pp. 1–7).