

MINIMALISTIC CYBER SECURITY FRAMEWORK (MCSF): A BRIDGE  
FRAMEWORK FOR SMALL BUSINESSES

by

TONY PAPA ADU FRIMPONG, MBA

Supervised by

SAGAR BANSAL, DBA

DISSERTATION

Presented to the Swiss School of Business and Management Geneva

In Partial Fulfillment

Of the Requirements

For the Degree

DOCTOR OF BUSINESS ADMINISTRATION

SWISS SCHOOL OF BUSINESS AND MANAGEMENT GENEVA

JANUARY, 2025

MINIMALISTIC CYBER SECURITY FRAMEWORK (MCSF): A BRIDGE  
FRAMEWORK FOR SMALL BUSINESSES

by

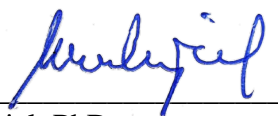
TONY PAPA ADU FRIMPONG, MBA

Supervised by

SAGAR BANSAL, DBA

APPROVED BY

dr. Jaka Vadnjal

  
Dissertation chair: Jaka Vadnjal, PhD.

RECEIVED/APPROVED BY:

\_\_\_\_\_  
Admissions Director

### **Dedication**

To my ever-loving mother, who could not live to see her son fulfill his dream of becoming a doctor: Mommy, I made it! Thank you for all the prayers.

## **Acknowledgments**

This dissertation would not have been possible without the unwavering support and guidance of my advisor, Dr. Sagar Bansal. Thank you for believing in me when I struggled to believe in myself. I would also take the opportunity to thank Dr. Raveena Chhabrani for her assistance as the editor.

I would also like to express my gratitude to my dad, who consistently encouraged me throughout this process with the question, "Are you done yet?" Now I can finally say, "Yes, Dad! I am done."

Most importantly, I want to thank my wife and kids for their patience and support during this journey. Their unconditional love and encouragement have meant the world to me.

Lastly, I want to acknowledge the friends I made along the way. Regardless of the experiences - good or bad - these beautiful friendships were instrumental in making this effort a success.

## ABSTRACT

### MINIMALISTIC CYBER SECURITY FRAMEWORK (MCSF): A BRIDGE FRAMEWORK FOR SMALL BUSINESSES

by

TONY PAPA ADU FRIMPONG  
JANUARY, 2025

Dissertation Chair: Jaka Vadjal, PhD.

Small businesses face significant cybersecurity challenges, often lacking the resources, expertise, and awareness required to mitigate risks effectively. This doctoral thesis investigates these challenges and provides practical solutions through the development and validation of the Minimalistic Cyber Security Framework (MCSF).

The research began by evaluating the existing awareness of cybersecurity risks among small business owners. Surveys revealed moderate awareness of basic threats such as phishing and malware, but a critical underestimation of complex risks like ransomware and insider attacks. Subsequently, the study examined common cybersecurity practices, finding heavy reliance on basic protections like antivirus software and firewalls, with minimal adoption of advanced measures such as multi-factor authentication or employee training. Barriers such as limited budgets, lack of technical expertise, and perceptions of low risk emerged as key impediments.

To address these issues, the study explored established cybersecurity frameworks, including the NIST Cybersecurity Framework and ISO/IEC 27001. These frameworks, while comprehensive, proved challenging for small businesses due to their complexity and resource demands. Using grounded theory, a streamlined Minimalistic Cyber Security

Framework was developed. This framework focuses on simplicity, modularity, and practicality, enabling small businesses to incrementally strengthen their cybersecurity posture.

Training programs and expert consultations were integral to the study. Tailored training sessions provided hands-on, relatable guidance, significantly improving participants' awareness and readiness to adopt cybersecurity measures. Personalized consultations ensured the framework could be adapted to individual business needs, fostering independent implementation and sustainability.

This thesis highlights critical gaps in small business cybersecurity and offers actionable, scalable solutions. By emphasizing accessibility and practicality, it paves the way for resource-constrained businesses to achieve robust cybersecurity resilience.

## TABLE OF CONTENTS

CHAPTER I: INTRODUCTION.....	1
1.1 Overview of Cybersecurity for Small Businesses .....	1
1.2 Cybersecurity Risks and Threats .....	4
1.3 Frameworks & Policies.....	6
1.4 Technologies and Solutions .....	9
1.5 Cybersecurity Management and Strategy .....	12
1.6 Cybersecurity Culture and Awareness.....	14
1.7 Financial and Economic Aspects .....	16
1.8 Research Problem & Question.....	18
1.9 Research Objectives.....	19
1.10 Research Limitations & Significance .....	20
CHAPTER II: LITERATURE REVIEW .....	23
2.1 General Overview of Cybersecurity Frameworks .....	23
2.2 NIST Cybersecurity Framework (CSF).....	26
2.3 ISO/IEC 27001.....	28
2.4 CIS Controls.....	31
2.5 COBIT.....	33
2.6 Risk Management Framework (RMF).....	36
2.7 ISO/IEC 27005.....	38
2.8 NIST Privacy Framework.....	39
2.9 Comparing and Integrating Frameworks .....	41
2.10 Gaps in Existing Literature .....	42
CHAPTER III: METHODOLOGY .....	45
3.1 Research Design.....	45
3.2 Rationale for Choosing Mixed-Methods Approach.....	46
3.3 Initial Survey and Descriptives Analysis.....	47
3.4 First Intervention by Researcher – 1 Month Training .....	48
3.5 Post Training Survey.....	49
3.6 Second Intervention by Researcher – 6 Months Consultations .....	50
3.7 Post-Consultation Interview & Thematic Analysis .....	51
3.8 Framework Development Using Grounded Theory .....	52
3.9 Validation Interview .....	53
3.10 Ethical Considerations: .....	54
CHAPTER IV: RESULTS.....	56
4.1 Cybersecurity Awareness Among Small Businesses.....	56
4.2 Small Business of Cybersecurity Frameworks After Training.....	58

4.3 Thematic Analysis of Post-Consultation Interviews.....	60
4.3.1 Overwhelming Complexity of Frameworks .....	61
4.3.2 Insufficient Resources and Know-How .....	62
4.3.3 Misalignment with Startup Priorities .....	62
4.3.4 Limited Applicability.....	63
4.3.5 Cybersecurity as Non-Essential Function.....	63
4.3.6 High Cost of Full Implementation .....	64
4.3.7 Temporary vs. Sustainable Security Practices .....	64
4.4 Development of a Minimalistic Cyber Security Framework .....	66
4.4.1 Risk Management Strategy Template .....	67
4.4.2 Asset Register Template .....	69
4.4.3 Common Controls List.....	72
4.4.4 Information Types for System Categorization List .....	74
4.4.5 Risk Register Template.....	76
4.5 Thematic Analysis of Interviews on the MCSF.....	79
4.5.1 Enhanced Accessibility and Comprehension.....	80
4.5.2 Practical Implementation with Limited Resources .....	80
4.5.3 Effective Risk Management.....	81
4.5.4 Improved Cybersecurity Posture.....	81
4.5.5 Empowerment and Independence .....	82
4.5.6 Alignment with Business Priorities .....	82
 CHAPTER V: CONCLUSIONS & RECOMENDATIONS .....	 84
5.1 Summary of Findings.....	84
5.2 Addressing the Research Objective .....	86
5.3 Recommendations.....	89
5.3.1 Policy Recommendations.....	90
5.3.2 Framework Adoption Strategies .....	90
5.3.3 Training and Education Initiatives.....	91
5.3.4 Enhancing Public Awareness and Community Engagement.....	91
5.3.5 Future Research and Development .....	92
5.4 Limitations of the Study.....	92
5.4.1 Geographical Scope .....	93
5.4.2 Evolving Cybersecurity Threats .....	93
5.4.3 Resource Constraints of Participants .....	94
5.4.4 Diversity and Size of the Sample.....	94
5.4.5 Methodological Choices .....	94
5.4.6 Focus on Specific Frameworks .....	95
5.5 Final Thoughts .....	95
5.5.2 A Call for Continued Engagement and Collaboration.....	96
5.5.3 Bridging the Knowledge and Resource Gap.....	96
5.5.4 The Road Ahead: Embracing Innovation and Agility .....	97
5.5.5 Emphasizing a Shared Responsibility.....	97



APPENDIX A: SURVEY QUESTIONS FOR UNDERSTANDING CYBERSECURITY AWARENESS AND READINESS AMONG SMALL BUSINESS OWNERS.....	99
APPENDIX B: SURVEY QUESTIONS FOR ASSESSING SMALL BUSINESS UNDERSTANDING AND IMPLEMENTATION OF CYBERSECURITY FRAMEWORKS AFTER TRAINING FOR 1 MONTH.....	106
APPENDIX C: INTERVIEW GUIDE FOR POST 3 MONTH CONSULTING ON CSF IMPLEMENTATION IN SMALL BUSINESSES .....	113
APPENDIX D: RISK MANAGEMENT STRATEGY TEMPLATE.....	117
APPENDIX E: ASSET REGISTER TEMPLATE.....	121
APPENDIX F: COMMON CONTROLS LIST .....	122
APPENDIX G: INFORMATION TYPES LIST .....	126
APPENDIX H: RISK REGISTER TEMPLATE.....	130
APPENDIX I: INTERVIEW GUIDE TO ASSESS THE SUCCESS OF MCSF .....	132
REFERENCES .....	140

## LIST OF FIGURES

Figure 3a: Illustration of Research Design Phases, Source: (Original Work) .....	46
Figure 4a: Structure of The Minimalistic Cyber Security Framework (MCSF), Source: (Original Work) .....	66
Figure 4b: MCSF Asset Register Template Structure, Source: (Original Work) .....	70
Figure 4c: MCSF Common Controls List Structure, Source: (Original Work).....	72
Figure 4d: MCSF Information Types List Structure, Source: (Original Work) .....	75
Figure 4e: MCSF Risk Register Structure, Source: (Original Work).....	76

## CHAPTER I: INTRODUCTION

This chapter provides an in-depth analysis of cybersecurity challenges faced by small businesses. It underscores the unique vulnerabilities of these enterprises, often characterized by limited resources, lack of technical expertise, and insufficient security measures. The discussion addresses the various cyber threats that small businesses encounter, such as phishing, ransomware, and insider threats, emphasizing the necessity for enhanced cybersecurity practices. By focusing on industry-specific risks, financial constraints, and the need for a proactive cybersecurity culture, this chapter sets the stage for understanding the broader cybersecurity landscape applicable to small enterprises. Through an analytical approach and the use of case studies, readers gain a nuanced perspective on the challenges that prevent small enterprises from implementing effective cybersecurity measures.

### **1.1 Overview of Cybersecurity for Small Businesses**

Small businesses often face tough hurdles when it comes to cybersecurity. Rapid advancements in technology, limited resources, and a lack of specialized knowledge make it difficult for them to implement effective security measures. Many focus only on basic protections, unintentionally neglecting crucial areas like threat detection, response, and recovery (Chidukwani et al., 2022). High costs of advanced cybersecurity solutions add to the challenge, leaving small businesses struggling to keep up with the constantly evolving threat landscape (Junior .J.C. et al., 2023). Despite these difficulties, small businesses do have some advantages. Their agility and flexible IT setups can be leveraged to enhance their security posture when approached strategically (Tam et al., 2021).

Unlike larger organizations, which typically have well-established cybersecurity frameworks, small businesses often operate with limited expertise in this area. Owners and

managers usually juggle multiple responsibilities, making it hard to dedicate time and resources to cybersecurity (Berry & Berry, 2018). Many lack formal policies and procedures, as well as trained IT staff, leaving their systems exposed to potential breaches (Tam et al., 2021). Larger companies, by comparison, are better equipped with resources and skilled teams to handle these challenges effectively.

Small businesses also face a wide range of threats, including viruses, ransomware, phishing scams, and malware (Thomas Hayes et al., 2012). As their reliance on digital platforms grows, risks like data breaches and phishing attacks become even more pressing (Abhiram et al., 2023). Emerging risks, such as vulnerabilities in wireless networks, challenges with cloud computing, and spear phishing attacks, are especially hard for small businesses to manage due to their limited expertise (Hutchings, 2012). Without sufficient resources to counter these threats, they face the possibility of severe financial losses and long-term reputational damage (Sangani & Vijayakumar, 2012).

Cybercriminals frequently target small businesses because they are seen as easy prey. With fewer financial resources, weaker security systems, and often overburdened IT teams, these organizations become prime targets (Alshboul & Streff, 2015). Many small businesses handle sensitive customer data but fail to implement strong safeguards, making them even more attractive to attackers (Imsand et al., 2019). On top of this, some business owners underestimate the risks, often due to a lack of awareness about the potential impact of cyber threats. The increasing complexity of legal and regulatory requirements only adds to the pressure, as businesses can face penalties or liabilities following a cyberattack (Selznick & Lamacchia, 2018).

For small businesses, cybersecurity is essential to ensure smooth operations and long-term survival. Cyberattacks or data breaches can disrupt daily operations, cause significant financial losses, and harm relationships with customers. To minimize these

risks, small businesses should include cybersecurity in their overall business continuity plans (Safa Altaha & Mohammad Sohel Rahman, 2023).

Proactive planning involves identifying potential threats, implementing preventive measures, and preparing for how to respond to an attack (Phillips & Tanner, 2019). Creating a culture of security awareness within the organization, securing buy-in from leadership, and providing regular training for employees can make a big difference.

A cybersecurity breach can be financially devastating for small businesses. Reports show that the average cost of a data breach was \$3.86 million in 2018—an amount that could bankrupt most small businesses (Knauer, 2019). Even a smaller financial hit can threaten the survival of these organizations. In the U.S. alone, businesses suffer \$67.2 billion in annual losses due to cybercrime, with an average loss of \$24,000 per company (Stevens, 2007). Beyond immediate costs, breaches can damage a business's reputation, straining relationships with customers, suppliers, and partners (Furnell et al., 2020).

Several obstacles make it difficult for small businesses to adopt strong cybersecurity practices. These include limited awareness of the risks, budget constraints, and a lack of technical expertise (Junior C.J. et al., 2023). Many owners view cybersecurity as a low-priority expense, focusing instead on day-to-day operations. In addition, undertrained IT staff and a lack of comprehensive policies and procedures for securing information resources contribute to the vulnerabilities faced by small businesses (Berry & Berry, 2018). Basic steps like using strong passwords and encrypting sensitive data are often overlooked due to time constraints or a lack of understanding (Imsand et al., 2019). This lack of preparedness leaves small businesses highly vulnerable to cyber threats.

Cybersecurity risks can vary significantly across industries. While all small businesses are susceptible to threats like phishing, malware, and ransomware, certain sectors face unique risks. For example, healthcare organizations are more prone to data

breaches because of the sensitive nature of patient records, while retail businesses often deal with payment card fraud (Kandpal et al., 2023). Regardless of the industry, many small businesses fall short when it comes to implementing adequate security measures. Addressing these risks requires a combination of comprehensive cybersecurity policies, regular training, and investments in advanced technology (Bamidele et al., 2024).

Small businesses' views on cybersecurity are shaped by factors like budget limitations, competing priorities, and external pressures (Kabanda et al., 2018). While some understand its importance, many see cybersecurity as secondary compared to other operational concerns (Teymourlouei & Harris, 2019). This mindset often results in underinvestment in cybersecurity, leaving businesses vulnerable. To address this, small businesses need to adopt a proactive approach, treating cybersecurity as a core part of their operations rather than an afterthought (Pickering et al., 2023).

## **1.2 Cybersecurity Risks and Threats**

Small businesses frequently face cyberattacks such as phishing, ransomware, malware, and insider threats. These organizations often struggle to defend against these threats, making it essential to strengthen cybersecurity measures to prevent financial losses, reputational harm, and legal complications.

Cybercriminals exploit vulnerabilities in small business IT infrastructures using social engineering tactics like phishing, baiting, and pretexting. These methods manipulate human behavior to gain access to sensitive information (Olaniyan & Ogunola, 2024). Limited resources and weak security practices make small businesses particularly vulnerable to these attacks. The shift to remote work during the COVID-19 pandemic further exposed these organizations to risks, often stemming from human error (Ncubukezi,

2022). Key measures such as employee training, multi-factor authentication, and strong endpoint protection are vital for mitigating these threats (Olaniyan & Ogunola, 2024).

Phishing attacks often trick employees into revealing confidential information, which can result in data loss or financial setbacks (Chaithanya & Brahmananda, 2021). Ransomware, which locks access to company data until a ransom is paid, and malware, which compromises entire systems, are especially harmful. A survey of UK-based SMEs highlighted that while many acknowledged the potential severity of cyberattacks, they underestimated the likelihood of these threats (Wilson et al., 2022). Traditional defenses alone are no longer sufficient, necessitating the use of advanced technologies like machine learning to identify malicious URLs and other threats (Chaithanya & Brahmananda, 2021).

Insider threats are another significant concern for small businesses. These threats can arise from employees acting maliciously or negligently, leading to severe security breaches. Incidents such as data theft or sabotage are particularly damaging (Moneva & Leukfeldt, 2023). Financial and ICT SMEs are especially at risk due to the sensitive nature of their data (Yeboah-Boateng, 2013). To combat insider threats, businesses should implement multi-layered defense strategies, including employee activity monitoring, regular audits, and caution with granting privileges to users (Omar, 2015).

Managing vulnerabilities and applying security patches remain challenging for small businesses. Many lack the expertise needed to stay current with vulnerability management, leaving them exposed to potential exploitation. While basic security tools like antivirus software may be in use, comprehensive security policies are often missing (Berry & Berry, 2018; Rohn et al., 2016). Delays in detecting and addressing vulnerabilities only increase the risk of successful cyberattacks.

Small businesses also struggle to effectively detect and respond to cybersecurity incidents. Many SMEs experience cyberattacks and data breaches annually, yet their

incident handling capabilities are frequently inadequate (Oluwadamilola Ogunyebi et al., 2018). Due to limited resources, these organizations focus more on preventing attacks than on detection and response (Alladukwani et al., 2022). Enhancing incident response plans and providing employees with cybersecurity education are critical steps to improve response times and minimize damage.

The consequences of cybersecurity breaches for small businesses can be severe, ranging from financial losses and operational disruptions to reputational harm. Financially, these breaches lead to increased expenses, while the reputational damage can have long-lasting effects. Interestingly, in some consumer-facing industries, smaller breaches may unexpectedly boost reputation, contrary to traditional assumptions (Makridis, 2020). The legal ramifications are equally significant, as businesses increasingly face penalties and lawsuits resulting from cybercrimes (Selznick & Lamacchia, 2018). Without strong legal frameworks, small businesses are often exposed to considerable liability if they fail to secure their data adequately.

Despite the frequent targeting of small businesses by cybercriminals, legal protections for these organizations are often insufficient (Tam et al., 2021). Courts and legislatures are increasingly permitting civil suits against companies that fall victim to cybercrimes (Selznick & Lamacchia, 2018). To reduce legal liability, small businesses must establish clear cybersecurity policies, yet many remain unaware of these legal risks and lack the necessary infrastructure to address them (Mitchell & Jones, 2002). Developing robust policies and providing ongoing cybersecurity training are essential steps in mitigating these risks.

### **1.3 Frameworks & Policies**



Implementing appropriate cybersecurity frameworks is essential for small businesses to strengthen their defenses. While the NIST Cybersecurity Framework is widely used, it may not fully address the unique needs of smaller enterprises. Researchers have proposed alternative frameworks such as the CyberSecurity Readiness Model for SMEs (CSRM-SME) and the Adaptable Security Maturity Assessment and Standardisation (ASMAS), which cater specifically to the challenges faced by small businesses (Wan Nur Eliana Wan Mohd Ludin et al., 2024). Simplified models emphasizing core cybersecurity principles have also proven effective, allowing small enterprises to bolster their security measures without straining their limited resources (Asprion et al., 2023).

Despite these advancements, many small businesses struggle to adopt comprehensive security policies and practices. Limited technical knowledge and budgetary constraints often result in reliance on basic security measures that fail to address more complex threats (Berry & Berry, 2018; Tam et al., 2021). This highlights the need for tailored solutions, including robust risk management strategies, incident response planning, and employee training. Customized awareness programs that incorporate behavioral psychology, practical scenarios, and AI-enhanced learning tools have been successful in fostering a strong security culture among employees (Friday Ugbebor et al., 2024). However, for such initiatives to succeed, management must demonstrate commitment and allocate sufficient resources.

One effective strategy for small businesses is adopting multi-factor authentication (MFA), which significantly improves defenses against phishing and other credential-based attacks. MFA is particularly crucial for SMEs using cloud services, as it strengthens authentication processes against evolving cyber threats (Zulkifli et al., 2023). Compliance with regulations like GDPR and HIPAA further underscores the importance of integrating

MFA into cybersecurity strategies to safeguard sensitive data while meeting legal requirements (Alimzhanova et al., 2024).

The General Data Protection Regulation (GDPR), designed to enhance data protection and privacy, poses unique challenges for small businesses. Compliance often demands significant investments in time, resources, and expertise, creating a competitive disadvantage compared to larger organizations (Wilkinson, 2018). Additionally, GDPR-related changes, such as restrictions on WHOIS data, have inadvertently impacted cybersecurity operations, prompting calls for more balanced regulatory frameworks (Ferrante, 2018). Addressing these challenges requires organizational commitment and external support through tailored consulting and regulatory guidance.

Navigating industry-specific regulations adds complexity to cybersecurity efforts, particularly in sectors like finance. Legal requirements, such as those under the Gramm-Leach-Bliley Act or the Sarbanes-Oxley Act, enforce strict standards on data protection and ethical practices (Mohammed, 2015). While compliance can be daunting, small businesses can leverage their agility and fragmented IT systems to adapt more efficiently to these demands (Tam et al., 2021). However, this potential is often underutilized, emphasizing the need for further research and policy development.

Third-party vendors and partner relationships introduce additional vulnerabilities, particularly within supply chains. Risks such as data breaches and weak security controls demand rigorous assessments, regular monitoring, and well-defined contractual agreements (Oluwatosin Ilori et al., 2024). For SMEs, integrating third-party risk management into their cybersecurity strategies is critical to reducing exposure and ensuring business continuity.

Cybersecurity insurance has become a valuable tool for managing risks, and providing financial coverage for cyber incidents. However, adoption among SMEs remains

low, often due to a limited understanding of cyber risks and the complexity of insurance policies (Adriko & Nurse, 2024). Government intervention and improved risk assessment frameworks could help encourage broader adoption, enabling small businesses to better manage their exposure to digital threats and minimize financial losses.

To address these multifaceted challenges, small businesses must adopt a proactive and comprehensive approach to cybersecurity. By implementing tailored frameworks, enhancing employee awareness, and leveraging tools like MFA and cyber insurance, they can protect their operations and build resilience in an increasingly digital world.

#### **1.4 Technologies and Solutions**

Cybersecurity technologies such as firewalls and anti-malware software are essential for small businesses, providing critical protection against malicious attacks. However, factors like budget constraints, vendor support, and awareness of potential threats significantly influence the adoption of these technologies by small and medium-sized enterprises (SMEs) (Lee & Larsen, 2009). Despite their importance, many small businesses neglect basic security measures, leaving themselves vulnerable to substantial risks (Ryan & Donnell, 2000). Effective cybersecurity strategies must combine technology, employee awareness, and external support to ensure comprehensive protection (Cook, 2017).

The rise of cloud computing has enabled small businesses to address resource limitations while improving cybersecurity. Cloud-based solutions offer cost efficiency, scalability, and advanced features like real-time threat detection and centralized management (Karagozlu et al., 2020; Ravuri et al., 2023). However, concerns regarding data confidentiality, integrity, and compliance remain significant challenges. To address these risks, small businesses must adopt robust security policies, including data encryption

and adherence to regulatory requirements (Karadsheh & Al Hawari, 2011). With proper safeguards in place, cloud solutions offer a practical way for resource-constrained businesses to strengthen their cybersecurity posture (Ravuri et al., 2023).

Integrating cybersecurity into IT infrastructure is often a complex task for small businesses. Many SMEs lack the technical expertise and resources needed to implement robust systems, frequently prioritizing other operational needs over security (Tam et al., 2024). Simplified models, such as the Small IT Data UML class model, provide practical frameworks to guide decision-making without unnecessary complexity (Tam et al., 2024). Additionally, the agility and modular nature of small business IT systems can be leveraged to create more resilient infrastructures (Tam et al., 2021). However, continued research and tailored policy development are vital to address the unique challenges faced by this sector.

Remote work and mobile device security present additional challenges, particularly for businesses with limited IT budgets and expertise. Key measures, such as multi-factor authentication (MFA), virtual private networks (VPNs), and regular software updates, are crucial for securing remote work environments (Manda, 2020). Innovations like Lightweight Portable Security (LPS) devices and Zero Trust Architecture offer advanced solutions that enhance security without overburdening resources (Coruh et al., 2021). Employee training also plays a critical role in mitigating risks from phishing and social engineering attacks, ensuring a secure and adaptable remote work environment (Manda, 2020).

Automation has become a pivotal aspect of cybersecurity for small businesses, particularly through intrusion detection systems (IDS). Advanced machine learning and deep learning-based IDS enable accurate and efficient threat detection at a fraction of the cost of traditional systems (Mudau et al., 2024). Cost-effective options, such as Raspberry Pi-based systems running tools like Snort or Suricata, allow SMEs to implement robust

security measures without significant financial strain (Cruz de la Cruz et al., 2020). Automated systems not only improve detection accuracy but also offer scalability and adaptability, making them indispensable for small businesses operating with limited resources (Mudau et al., 2024).

Balancing cybersecurity investments with financial constraints remains a persistent challenge for SMEs. Many lack formalized processes for budget allocation, which limits their ability to implement effective strategies (Heidt & Gerlach, 2018). Decision-support frameworks like CENSOR help businesses optimize investments by balancing risk and cost (Tsiodra et al., 2023). Research shows that industry-specific approaches are necessary, with sectors like finance and technology allocating higher budgets to address their unique risks (Zhuo & Solak, 2015). These targeted strategies ensure that small businesses can maximize the impact of their limited resources.

Securing an online presence is critical for small businesses operating in the digital economy. Effective strategies include aligning website content with business objectives while implementing robust cybersecurity measures to prevent attacks (Burgess, 2009; Rahman & Lackey, 2013). Data-driven decision-making and a focus on customer experience enable small businesses to remain competitive in the digital marketplace (Hameed et al., 2021). Additionally, compliance with privacy and fair trading regulations helps build customer trust and ensures legal protection (Shelly & Jackson, 2009).

Protecting customer data, especially in e-commerce settings, is a significant concern for small businesses. Many handle sensitive information without adequate security measures, exposing themselves to legal and reputational risks (Batten & Castleman, 2005). Governments and larger trading partners can play a critical role by providing resources, training, and incentives to encourage small businesses to adopt best practices in data security (Williams & Manheke, 2010). By establishing strong IT security policies and

adhering to legal requirements, small businesses can safeguard their operations and build lasting trust with their customers.

### **1.5 Cybersecurity Management and Strategy**

Research shows that multi-criteria decision-making techniques, like the best-worst method, can help small businesses allocate their resources more effectively (Alva Hendi Muhammad et al., 2023). Cybersecurity plans that include monitoring infrastructure and training employees are particularly effective. However, many small businesses still lack comprehensive strategies (Haydar Teymourlouei & Vareva E. Harris, 2019). Awareness remains a critical yet under-researched aspect, pointing to the need for more targeted studies to close this gap (Sunil Chaudhary et al., 2023).

Contrary to the belief that increased spending automatically results in better security, research reveals that strategic allocation of resources often produces superior outcomes. For example, the CENSOR framework offers small businesses a decision-support tool that helps them manage risks effectively within budget constraints (Maria Tsiodra et al., 2023). This highlights the importance of informed investment and strategic decision-making rather than focusing solely on expenditure.

Small businesses require customized approaches to assess and manage risks, considering their unique challenges and operational realities. While many business owners use basic risk management tools, they often lack comprehensive policies and regular training (Berry & Berry, 2018). Tailored threat assessments that promote autonomy and competence can encourage action in small business environments (van Haastrecht et al., 2021). Risk categorization frameworks, which focus on security, dependency, and legal risks, provide practical ways for smaller enterprises to navigate the complexities of cybersecurity (Sukumar et al., 2023).

Proactive management strategies have become essential as cyber threats continue to grow. Comprehensive policies, employee training, and advanced technologies are critical for improving preparedness (Lucky Bamidele et al., 2024). The pandemic highlighted weaknesses in IT security, emphasizing the importance of ongoing monitoring and strategic planning (Yakubu AjijiMakeri, 2020). Trends like AI-driven threat detection and collaborations between small businesses and cybersecurity firms underline the value of innovation and partnerships in enhancing resilience (Lucky Bamidele et al., 2024). Building a culture focused on cybersecurity within organizations can lead to long-term benefits.

Incident response planning is also key to managing breaches effectively. Industries such as hospitality face frequent attacks, underscoring the need for tailored frameworks to address these issues (Oluwadamilola Ogunyebi et al., 2018). Effective incident response involves preparation, including creating policies, conducting training, and running regular drills (Bareja, 2021). For resource-limited businesses, outsourcing incident management can be a practical solution, provided vendors are chosen with due diligence.

Collaboration with external experts can significantly enhance internal efforts. Research highlights the effectiveness of relying on high-quality external expertise rather than traditional management support for implementing robust information systems (Thong et al., 1996). Small businesses often use reactive or ad hoc strategies to access expertise, but structured collaborations that involve shared responsibilities have proven more effective (Viljamaa, 2011; Mmango & Gundu, 2024). These partnerships strengthen resilience by fostering collective knowledge and aligning small businesses with broader industry and government support.

Implementing cybersecurity policies in diverse small business environments remains a persistent challenge. Limited resources, fragmented IT systems, and a lack of

expertise often hinder progress (Chidukwani et al., 2022). Many existing frameworks are not suitable for small enterprises, highlighting the need for more adaptable solutions (Pawar & Palivela, 2022). However, the flexibility and agility of small businesses can be leveraged as advantages when properly utilized (Tam et al., 2021). Addressing these challenges will require ongoing research, effective policies, and external support to build a sustainable cybersecurity ecosystem for small enterprises.

To meet the evolving demands of cybersecurity while maintaining their operational focus, small businesses must continue to explore innovative solutions and participate in targeted initiatives.

## **1.6 Cybersecurity Culture and Awareness**

Small businesses are essential to the global economy, yet their vulnerability to cyber threats is the main concern. Limited resources and expertise make fostering a cybersecurity culture both challenging and necessary. A significant obstacle is the lack of awareness among many small business owners, who often fail to recognize the importance of cybersecurity until faced with a direct threat. Risk analyses have proven effective in demonstrating the value of proactive measures (Dojkovski et al., 2006; Dojkovski, 2017).

Strong leadership is critical for cultivating a robust cybersecurity culture. Without management's commitment and formalized policies, efforts often fall short. Businesses must implement structured training programs that go beyond technical knowledge, fostering accountability and active employee engagement (De Silva, 2023). Tailored training for SMEs has been shown to reduce incidents caused by human error, which is a leading vulnerability in most organizations (Ugbebor et al., 2024). Building trust in culturally diverse workplaces is also essential, as unresolved trust issues can inadvertently increase cybersecurity risks (Gundu et al., 2019).



Financial constraints often limit small businesses' ability to implement advanced cybersecurity measures. However, these challenges can be mitigated by partnering with IT providers and government organizations that offer accessible and context-specific solutions. IT companies play a crucial role in bridging the gap between small businesses and the latest cybersecurity practices. Nevertheless, these companies also face their own resource constraints and varying levels of expertise, which can impact the quality of their support (Cartwright et al., 2023).

Employee behavior is another critical factor in cybersecurity success. Motivating employees to follow best practices requires a balance of mandatory policies and intrinsic motivators. Tools like CYSEC, based on the Self-Determination Theory, address employee autonomy, competence, and relatedness, helping small businesses implement secure practices that align with their operational needs (Shojaifar et al., 2020; van Haastrecht et al., 2021).

When designed effectively, cybersecurity education can transform from a formality into a key asset for SMEs. Practical, engaging training programs tailored to the resources and structures of small businesses are most effective. By integrating principles of behavioral psychology and hands-on application, these programs help employees understand and internalize cybersecurity practices (Tracy Tam et al., 2021). Management support and reinforcement of learned behaviors further enhance their effectiveness (Friday Ugbebor et al., 2024).

Despite these advancements, challenges remain. The evolving nature of cyber threats requires ongoing research and refinement of training methodologies. Tailored solutions addressing specific business models and IT environments are essential for improving resilience across the SME sector. Collaboration among practitioners,

policymakers, and the IT community will be key to developing scalable solutions that empower small businesses to protect themselves against cyber risks (Kabanda et al., 2018).

In summary, achieving robust cybersecurity in small businesses requires a holistic approach combining technical solutions, cultural adaptation, and human-centered strategies. By fostering a shared sense of responsibility, small businesses can protect their operations while contributing to a safer digital ecosystem.

### **1.7 Financial and Economic Aspects**

Small businesses, especially technology startups, often face difficulties in measuring the return on investment (ROI) in cybersecurity. To address this, Marican et al. (2023) developed an enhanced Return on Security Investment (ROSI) model designed specifically for startups. This model provides both minimum and maximum ROSI values, enabling businesses to fine-tune their cybersecurity spending based on their unique risks and needs. Onwubiko & Onwubiko (2019) highlighted the importance of using key performance indicators (KPIs) and metrics—such as the number of detected incidents or prevented attacks—to demonstrate ROI. Despite this, Moore et al. (2015) found that many companies skip ROI calculations, instead relying on strategic frameworks like NIST and COBIT. This tendency stems from executives' confidence that their firms are adequately funded for cybersecurity, even though hiring skilled personnel remains a persistent challenge.

Economic constraints also play a major role in hindering small businesses from adopting robust cybersecurity measures. Financial limitations, coupled with a lack of awareness and insufficient cybersecurity knowledge, create significant obstacles (Rombaldo Junior et al., 2023; Alahmari & Duncan, 2021). These challenges are compounded by immature organizational processes and weak legal frameworks, which

limit the effectiveness of cybersecurity efforts (Tam et al., 2021). Additionally, the absence of standardized risk frameworks and overconfidence among decision-makers exacerbate these issues (Alahmari & Duncan, 2021). While SME-focused research often emphasizes threat prevention, it frequently overlooks critical areas like detection, response, and recovery (Chidukwani et al., 2022). Nonetheless, certain characteristics of SMEs, such as agility and adaptable IT architectures, could support stronger cybersecurity practices if properly utilized (Tam et al., 2021).

To effectively evaluate cybersecurity investments, small businesses need structured methodologies that weigh costs against benefits. Frameworks like the SQUARE project enable hierarchical cost-benefit analysis by categorizing threats and assessing potential outcomes (Xie et al., 2004). Similarly, the Gordon-Loeb Model, when integrated with the NIST Cybersecurity Framework, helps businesses determine optimal spending levels and evaluate implementation strategies (Gordon et al., 2020). For long-term analysis, Net Present Value (NPV) can provide insights into the financial impact and sustainability of cybersecurity investments, particularly in securing supply chains (Ofori-Yeboah et al., 2021). Additionally, the CENSOR framework offers a comprehensive decision-support tool that considers factors like attack progression and budget constraints (Tsiodra et al., 2023). These methodologies emphasize that while spending is important, strategic allocation is key to achieving effective risk mitigation.

Recognizing the financial challenges faced by small businesses, governments, and organizations have introduced funding programs to support cybersecurity efforts. For example, the UK government offers a £5,000 grant to help small businesses strengthen their cyber defenses (Edmondson, 2015). Effective use of such funding includes monitoring IT infrastructure and developing detailed cybersecurity plans tailored to specific threats (Teymurlouei & Harris, 2019). These initiatives not only help mitigate

immediate risks but also contribute to creating governance frameworks that protect sensitive data and minimize business interruptions (Saha & Anwar, 2024).

The digital landscape continues to evolve, presenting new challenges for small businesses. Emerging threats such as AI-driven cyberattacks, vulnerabilities in IoT devices, and cryptocurrency-based crimes are becoming more prevalent (Patel & Rengarajan, 2024). Advanced technologies like AI, blockchain, and machine learning hold promise for addressing these challenges. AI-driven systems can detect and respond to threats in real time, while blockchain's decentralized and immutable design enhances data security (Familoni et al., 2024). However, implementation challenges, including high costs, skill shortages, and integration complexities, need to be resolved (Ogun & Olupinla, 2024). By leveraging government incentives, investing in workforce training, and collaborating with industry leaders, small businesses can overcome these barriers and improve their cybersecurity resilience.

The future of cybersecurity for small businesses will depend heavily on innovation and collaboration. While financial and organizational challenges remain significant, targeted research, strategic investments, and supportive initiatives can empower small businesses to adapt to the digital age and thrive despite the risks.

## **1.8 Research Problem & Question**

The research problem of this study is the inadequacy of existing cybersecurity frameworks to meet the specific constraints of small businesses. Small businesses are increasingly targeted by cybercriminals due to their perceived vulnerability, often lacking the sophisticated defense measures including dedicated IT resources as found in larger organizations. Despite their critical role in the global economy, these businesses typically

operate under significant resource limitations, including financial and technical expertise, which hinder their ability to implement comprehensive cybersecurity measures.

The primary research question guiding this study is: "How can a cybersecurity framework tailored to the specific needs and resource constraints of small businesses be developed and effectively implemented to enhance their cybersecurity posture?"

To address this overarching question, several sub-questions need to be explored:

- What are the current cybersecurity practices and awareness levels among small businesses?
- Which existing cybersecurity frameworks are deemed most applicable for small businesses, and what are the barriers to their adoption?
- How can small businesses be equipped with the knowledge and tools necessary to implement effective cybersecurity measures?
- What key elements should a minimalistic and practical cybersecurity framework for small businesses include?

## **1.9 Research Objectives**

The objective of this research is structured to systematically address the research problem and answer the research questions through a detailed and methodical approach.

They are as follows:

- Assess the existing awareness levels regarding cybersecurity risks and vulnerabilities.
- Investigate the common cybersecurity practices employed by small businesses.
- Explore which frameworks are most practical and applicable for small businesses to adopt.

- Identify the key obstacles small businesses face in implementing these frameworks.
- Create and deploy training programs to enhance cybersecurity awareness and facilitate framework adoption among small business owners.
- Offer expert consultations to customize cybersecurity measures that address the specific requirements of small businesses.
- Apply grounded theory to construct a simplified cybersecurity framework informed by practical insights.
- Validate the framework's effectiveness, usability, and impact in real-world small business scenarios.

### **1.10 Research Limitations & Significance**

While this study takes a comprehensive approach, certain limitations must be acknowledged to provide a well-rounded view of its findings and their applicability:

- **Geographical Scope:** The research focuses on small businesses within the United States, which may limit the applicability of its findings to regions with different regulatory frameworks, cultural norms, and cybersecurity challenges. Although perspectives from international experts were included to enhance the framework's relevance, global variations in cybersecurity landscapes could influence its broader applicability.
- **Evolving Cybersecurity Threats:** Cybersecurity is a dynamic field where new threats emerge continuously. The findings of this study reflect current threats and practices but may require adjustments to address future developments in the cybersecurity landscape.

- **Resource Constraints of Participants:** The small businesses involved in this study varied in their resource levels and technological capacities. This disparity may affect the adoption and effectiveness of the proposed framework. Businesses with minimal resources or different operational setups might not have their challenges fully captured.
- **Sample Size in Consultation Phase:** The consultation phase included only 25 small businesses, which, while necessary due to the intensive nature of the study, limits the diversity of insights across various sectors. This smaller sample size may impact the breadth of the study's applicability.

This research points out a critical gap in the literature by focusing on the development of cybersecurity frameworks specifically designed for small businesses. Through a mixed-methods approach, it provides a refined understanding of the cybersecurity challenges and practices unique to small enterprises. The framework developed from real-world data introduces a modest, practical approach to cybersecurity, contributing to the theoretical foundations of the field and serving as a model for future framework design. Moreover, the use of grounded theory underlines the value of qualitative methods in cybersecurity research, encouraging further academic exploration in this domain.

The actionable outcome depicts the significance of this study for small businesses. The Minimalistic Cybersecurity Framework (MCSF) developed in this research offers a tailored solution to the resource and operational constraints faced by small businesses. By emphasizing simplicity, accessibility, and cost-effectiveness, the framework equips small businesses with the tools to bolster their cybersecurity defenses without requiring substantial resources or technical expertise. The proposed interventions, including training and consultations, aim to enhance resilience against cyber threats, protect sensitive data,

and ensure business continuity. By simplifying complex cybersecurity frameworks and fostering a culture of security awareness, the study empowers small businesses to navigate the cybersecurity landscape with greater confidence.

This chapter has highlighted the significant challenges small businesses face in protecting their digital environments, reinforcing the urgent need for effective cybersecurity strategies. The discussion serves as a foundation for subsequent chapters, which will delve deeper into strategic solutions.

The next chapter, "Literature Review," will examine various cybersecurity frameworks, critically evaluating their applications and identifying barriers to their adoption by small businesses. This analysis guides the identification of adaptable frameworks, paving the way for developing a simple cybersecurity framework tailored to the specific needs of small enterprises.



## CHAPTER II: LITERATURE REVIEW

This chapter highlights a detailed review of the existing literature on the critical role of cybersecurity frameworks in managing digital risks across diverse organizational contexts. Frameworks such as the NIST Cybersecurity Framework, ISO/IEC 27001, COBIT, and CIS Controls play a crucial role in helping organizations strengthen their security measures. These frameworks offer structured guidance that encompasses key cybersecurity functions, including identification, protection, detection, response, and recovery. The discussion examines how these frameworks accommodate the specific requirements of different industries worldwide, emphasizing their adaptability and integration into organizational practices.

### **2.1 General Overview of Cybersecurity Frameworks**

Cybersecurity frameworks play a critical role in managing risks in today's digital world. Well-known frameworks such as the NIST Cybersecurity Framework, ISO/IEC 27001, COBIT, CIS Controls, and SANS Critical Security Controls provide structured guidance to help organizations secure their systems. These frameworks address essential cybersecurity functions, including identification, protection, detection, response, and recovery, and are designed to meet the needs of various industries. Notably, NIST SP 800-53 and ISO/IEC 27001:2013 are recognized for their comprehensive security controls and global relevance. These frameworks often serve as the foundation for hybrid models, which blend elements from multiple frameworks to address specific organizational requirements (Abassi Haji Juma et al., 2023; Kurii & Opirskyy, 2022).

Adopting these frameworks significantly improves an organization's security posture. The NIST methodology aligns cybersecurity risks with organizational objectives, while collaborative models like CyRLEC promote partnerships with law enforcement for

effective threat mitigation. Frameworks designed for specific environments, such as cloud computing, incorporate advanced technologies like machine learning to tackle unique challenges. ISO standards, particularly the ISO/IEC 27000 series, emphasize embedding cybersecurity into organizational culture, fostering comprehensive risk management and information security across various sectors (Mahn et al., 2021; Schiliro, 2023; Folorunso et al., 2024).

A comparative analysis of frameworks highlights their varied scopes and applications. For instance, while NIST SP 800-53 and ISO/IEC 27001 provide extensive coverage, national frameworks from countries like Australia, the UK, and the USA prioritize specific security domains. Industries such as finance and business process outsourcing often implement multiple frameworks to address regulatory and operational requirements. These comparisons help executives refine cybersecurity strategies by aligning them with industry-specific needs and compliance demands (Dedeke & Masterson, 2019; Blancaflor et al., 2023).

The distinction between prescriptive and risk-based approaches reveals the adaptability of cybersecurity strategies. Prescriptive frameworks offer predefined security measures that ensure consistency and reliability but may lack flexibility. Risk-based frameworks, on the other hand, focus on adapting to emerging threats through proactive analytics and stakeholder engagement. By combining these approaches, organizations can balance rigid compliance with dynamic risk management (Ladd & Lipner, 2012; Collier et al., 2014).

Compliance is another area where cybersecurity frameworks excel. Frameworks like SOC 2, GDPR, PCI DSS, and CMMC 2.0 provide structured paths to meet regulatory standards. However, achieving compliance alone is not sufficient for comprehensive cybersecurity. Organizations must complement compliance efforts with proactive

strategies, innovative technologies, and awareness of emerging threats to maintain strong defenses (Wenjia Wang et al., 2024; Madnick et al., 2019).

For small businesses, cybersecurity frameworks can be transformative. By integrating governance and risk mitigation practices at the management level, small enterprises can leverage their adaptability to secure digital assets and outpace larger competitors. Frameworks designed for smaller organizations prioritize simplicity and strategic development, enabling them to innovate and succeed in the cybersecurity domain (Lloyd, 2020; Asprion et al., 2023).

Emerging technologies like IoT and cloud computing have driven the evolution of cybersecurity frameworks. New models such as Adaptive Multi-Layer Security and Blockchain-Enabled Distributed Trust address the complexities of these technologies. These frameworks ensure that security measures are embedded at every level of IoT systems, providing robust solutions for increasingly interconnected environments (Chippagiri Srinivas, 2015; Pacheco et al., 2018).

Choosing the right framework involves careful consideration of factors such as cost, regulatory alignment, and organizational risk maturity. Incorporating cost-benefit analyses into frameworks like NIST helps optimize cybersecurity investments, ensuring alignment with business objectives and effective navigation of digital complexities (Gordon et al., 2020; Kissoon, 2020).

Despite their significance, cybersecurity frameworks face challenges, including the rapidly evolving threat landscape and the complexity of standardization. Frameworks like OSINT encounter issues with data quality and integration, requiring advanced tools and ethical practices to overcome these obstacles. As digital threats become more sophisticated, developing innovative AI-driven solutions is crucial to enhancing the effectiveness of these frameworks (Devu Govardhan et al., 2023; Abassi Haji Juma et al., 2023).

## **2.2 NIST Cybersecurity Framework (CSF)**

The NIST Cybersecurity Framework (CSF) is a practical tool designed to help organizations of all sizes manage cybersecurity risks effectively. Its flexible structure allows it to adapt to different industries, making it a valuable resource for enhancing security practices. The framework is built around five core functions: Identify, Protect, Detect, Respond, and Recover. These functions outline the key steps needed to manage cybersecurity risks while aligning with industry standards and best practices. This makes the CSF an accessible and reliable guide for improving an organization's security posture (Barrett, 2018; Dimitrov et al., 2021).

The "Identify" function forms the foundation of the framework by helping organizations understand their security environment. It includes activities like cataloging critical assets, assessing vulnerabilities, and identifying risks. These steps allow businesses to create a solid starting point for improving their cybersecurity measures (Gourisetti et al., 2019). Tools such as web-based CSF applications and the SME Cyber Security Evaluation Tool (CET) make this process easier by providing clear guidance and measurable insights. These tools are especially useful for sectors like critical infrastructure, small businesses, and local governments (Ibrahim et al., 2018; Benz & Chatterjee, 2020).

The "Protect" function focuses on safeguarding against potential threats by implementing proactive measures. It addresses areas like IT systems, cyber-physical networks, and Internet of Things (IoT) devices, emphasizing the importance of ongoing improvements and well-structured strategies. By fostering the adoption of best practices and clear policies, this function equips organizations with the resources needed to defend their systems effectively (Gourisetti et al., 2019; Saritac et al., 2022).

The "Detect" function is vital for identifying potential threats quickly to minimize their impact. By enabling proactive monitoring of environments, the CSF equips

organizations with tools and methodologies suited to modern cybersecurity challenges. This proactive approach is particularly critical for sectors like critical infrastructure, where operational continuity is paramount (Klien & Mohamed, 2022).

When cybersecurity incidents occur, the "Respond" function ensures that organizations can mitigate damage effectively. This function goes beyond immediate action, incorporating lessons learned to inform future improvements. By fostering clear communication across all organizational levels, it enhances coordination during crises and bolsters overall resilience (White & Sjelin, 2021; Ibrahim et al., 2018).

The "Recover" function focuses on restoring operations and learning from incidents to prepare for future threats. Recovery planning and continuous improvement are key aspects of this function. Case studies with local governments highlight how the framework provides actionable insights and recommendations for enhancing resilience (Ahmed Ibrahim et al., 2018).

The CSF's compatibility with other standards, such as ISO/IEC 27001, GDPR, and NIST SP 800-53, makes it even more valuable. This seamless integration allows organizations to align their cybersecurity initiatives with global best practices, leveraging multiple frameworks to address specific challenges (Almuhammadi & Alsaleh, 2017; Alghamdi, 2023). For instance, ISO/IEC 27001:2022 includes controls tailored for cloud computing, further demonstrating the CSF's relevance in today's cybersecurity landscape (Malatji, 2023).

For SMEs, the CSF provides an adaptable framework to enhance cybersecurity without requiring significant resources. Although limited expertise can be a challenge, adopting the CSF helps smaller organizations align with global standards and improve their security posture (Lubna Ambreen et al., 2024). Tools like sector-specific maturity models

and Baseline Tailor simplify the implementation process, making the framework accessible to organizations with diverse capabilities (Lubell, 2016).

The framework's flexibility is evident in its wide-ranging applications across industries. Organizations can tailor their implementation to suit their specific environments, ensuring both relevance and effectiveness. This adaptability, combined with its comprehensive approach, highlights the CSF's importance as a cornerstone of modern cybersecurity strategies (Parmar & Miles, 2024). By focusing on risk management, communication, and continuous improvement, the NIST Cybersecurity Framework remains an indispensable tool for overcoming the evolving challenges of cyber threats.

### **2.3 ISO/IEC 27001**

ISO/IEC 27001 is a key framework for establishing effective Information Security Management Systems (ISMS), meeting diverse organizational needs while promoting continuous improvement. Its structured approach to cybersecurity and risk management highlights a strong commitment to protecting information assets and ensuring business resilience.

The framework outlines 21 requirements, including seven mandatory and fourteen categorical elements, all guided by the Plan-Do-Check-Act (PDCA) cycle. This iterative method ensures a systematic approach to managing information security. Document management is a critical component, allowing organizations to track and control ISMS elements throughout their lifecycle effectively (Martelo et al., 2015). ISO/IEC 27001 also prioritizes human resources security, addressing risks while fostering compliance and external validation (Militaru, 2009).

A defining feature of ISO/IEC 27001 is its focus on continuous improvement. The framework emphasizes measuring ISMS effectiveness, using feedback from the PDCA

cycle to drive enhancements (Carvalho & Marques, 2019). Supporting standards like ISO/IEC 27004 provide tools for evaluating information security metrics, although smaller organizations may find these methodologies complex (Skaaland, 2008). Maturity models based on ISO/IEC 27001 help organizations assess their current capabilities and create customized improvement strategies (Proença & Borbinha, 2018).

At the heart of ISO/IEC 27001 is its approach to risk assessment and treatment. Organizations are required to identify vulnerabilities, evaluate potential threats, and implement targeted controls to mitigate risks effectively. This dynamic process demands careful decision-making and structured oversight, often managed by an Information Security Governance Team to ensure ongoing protection and risk management (Sassaman, 2020).

ISO/IEC 27001's adaptability extends to its integration with other quality management frameworks, such as ISO 9001. This integration streamlines management processes, reduces redundancies, and enhances overall efficiency. Common elements like document control and internal audits foster a unified approach to compliance and operational excellence (Chiang Wang & Dwen-Ren Tsai, 2009). Research emphasizes the importance of strategic resource allocation and addressing human factors for successful integration (Fiore et al., 2021).

The framework also supports compliance with global data protection laws, including the EU's General Data Protection Regulation (GDPR). By aligning with regulatory requirements, ISO/IEC 27001 helps organizations navigate complex legal environments. Complementary standards such as ISO/IEC 27701 further strengthen privacy management strategies by addressing specific requirements for data protection (Lopes et al., 2019; Anwar & Gill, 2020).

However, implementing ISO/IEC 27001 can pose challenges, especially for smaller organizations or those in developing regions. Barriers like limited resources, lack of awareness, and cultural resistance can hinder adoption. Simplified guides and tools tailored for SMEs help address these challenges, enabling resource-constrained organizations to benefit from the framework (Thierry Valdevit et al., 2009). Encouraging employee collaboration and incorporating familiar business practices further ease the transition, ensuring improved security and stakeholder trust (Coles-Kemp & Overill, 2007).

Leadership commitment is crucial for successful ISO/IEC 27001 implementation. Effective leadership ensures alignment of organizational priorities, provides adequate training, and cultivates a culture of continuous improvement (Fitroh et al., 2017). By adopting a comprehensive approach, organizations can safeguard the confidentiality, integrity, and availability of information while advancing their business objectives (Calder, 2009).

Choosing between ISO/IEC 27001 and other frameworks, such as the NIST Cybersecurity Framework, often depends on an organization's specific needs and strategic goals. While ISO/IEC 27001 emphasizes global applicability and a maturity model, the NIST CSF is more focused on critical infrastructure protection. Both frameworks aim to address cybersecurity challenges but differ in scope and implementation, offering flexibility for organizations to choose based on their unique requirements (Malatji, 2023).

Ultimately, ISO/IEC 27001 provides a solid foundation for managing information security in an ever-evolving digital landscape. Whether integrated with other standards, used for regulatory compliance, or applied to address vulnerabilities, its adaptability ensures relevance across industries and regions. By emphasizing systematic risk management and continuous improvement, ISO/IEC 27001 remains a vital tool for achieving long-term cybersecurity and information security objectives.



## 2.4 CIS Controls

The CIS Controls, created by the Center for Internet Security, offer a comprehensive framework for enhancing organizational cybersecurity. With 20 controls and 171 sub-controls, these guidelines are widely regarded as a critical tool for strengthening cyber defenses. However, debates continue around their practical implementation and effectiveness. Researchers like Gros (2019) call for more empirical validation, especially when comparing the CIS framework to other standards such as ISO, NIST, and PCI. Despite these critiques, CIS Controls remain a valuable resource in the cybersecurity field.

A key strength of CIS Controls is their emphasis on actionable security measures. Hnatienko and Tmenova (2020) recommend using mathematical models to rank these measures, allowing organizations to balance costs and risks effectively. Similarly, Asad Cue et al. (2024) introduced a scoring system in CIS Controls Version 8.0, which combines Rank-Weight methods with safeguard levels. This helps resource-limited organizations allocate their cybersecurity efforts efficiently, showcasing the framework's adaptability to diverse needs.

The "Basic CIS Controls" provide an essential starting point for organizations, offering a foundational layer of security akin to basic physical protections like locking doors (Blum, 2020). However, as Solms (1997) observes, these baselines are most effective when combined with comprehensive risk analysis and tailored measures. By focusing on fundamental practices, CIS Controls enable entities with limited resources to achieve sufficient security levels without requiring exhaustive assessments.

The CIS Controls also integrate seamlessly with other frameworks, enhancing their utility. For instance, Irawan et al. (2024) suggest combining the CIS Controls with the NIST Cybersecurity Framework (CSF) to create a maturity assessment model. This

integration allows organizations to align cybersecurity practices with strategic objectives, blending flexibility with rigor. Such mappings demonstrate how CIS Controls can complement established frameworks to build more robust security systems.

Small businesses, often constrained by limited budgets and expertise, stand to benefit significantly from the CIS Controls. These guidelines help smaller entities mitigate risks effectively while remaining cost-efficient. Paulsen (2016) highlights the potential for small enterprises to excel in cybersecurity by adopting proactive measures. Implementing the CIS Controls not only safeguards against data breaches and fraud but also fosters trust and operational resilience. Frameworks like CENSOR, proposed by Tsiodra et al. (2023), further simplify the process for smaller organizations by offering tailored, cost-effective strategies.

In incident detection and response, the CIS Controls demonstrate notable strengths. The framework integrates advanced tools like machine learning and threat intelligence systems to identify and address cyber threats in real time (Saravanakumar Baskaran, 2019). This reduces false positives and enhances response efficiency. Additionally, its adaptability to specialized settings, such as Industrial Control Systems (ICS), ensures its relevance across various industries (He & Janicke, 2015).

Despite their advantages, organizations often face challenges when implementing CIS Controls. Common obstacles include cultural resistance, limited resources, and the complexity of manual processes (Ambika P. H & Sujatha, 2024). Solutions such as automated compliance tools and cybersecurity intelligence-sharing practices can help overcome these barriers. Barcelos et al. (2024) stress the need to balance investments in technology with employee training to address internal resistance and improve overall readiness.

While challenges remain, the CIS Controls continue to serve as a cornerstone of modern cybersecurity. Their structured yet flexible approach helps organizations manage risks, improve cybersecurity maturity, and address skill gaps effectively. Although further research is needed to validate their full impact, the framework's adaptability ensures its ongoing relevance in an ever-changing threat landscape.

## **2.5 COBIT**

COBIT, or Control Objectives for Information and Related Technologies, is a renowned framework that bridges the gap between IT governance and cybersecurity. Its evolution reflects the increasing complexity of enterprise IT and the growing demand for robust cybersecurity measures. COBIT helps organizations effectively manage IT systems while ensuring alignment between IT strategies and business objectives. It encompasses key components like security governance, management, and assurance, enabling businesses to address systemic challenges and enhance cybersecurity practices (ISACA, 2013; Mangalaraj et al., 2014). Its adaptability is evident in how institutions, such as universities, have used COBIT to develop IT governance models tailored to their security and compliance needs (Abdulrasool & Turnbull, 2020).

One of COBIT's key strengths is its ability to align cybersecurity practices with broader business goals. By providing a structured approach to map business objectives with IT processes, COBIT helps organizations focus on critical areas like IT risk and service management (Hanafi et al., 2020). This alignment ensures that IT initiatives contribute directly to an organization's strategic vision, supported by COBIT's robust evaluation and monitoring mechanisms (Wijaya, 2023). When paired with complementary frameworks like ITIL, COBIT creates a solid foundation for achieving business-IT alignment while addressing both operational and technical concerns (Zeinolabedin et al., 2014).

In risk management, COBIT excels by offering detailed processes for managing enterprise IT risks and achieving regulatory compliance. Domains like APO12 and EDM03 provide clear guidelines for IT risk management audits (Handayani et al., 2023). COBIT also supports compliance with specific regulatory frameworks, such as the King III Report (Steenkamp, 2011). Simplified tools like "COBIT 5 for Risk" enable organizations to assess IT governance maturity and refine their strategies to manage risks effectively (Berrada et al., 2021).

COBIT also shines in addressing information security and privacy risks. By aligning with international standards like ISO/IEC 27001, it provides a roadmap for implementing effective information security measures (Sheikhpour & Modiri, 2012). While COBIT 5 delivers comprehensive guidelines for managing information security risks, its high-level focus may require supplementary tools for detailed implementation (Al-Ahmad & Mohammed, 2015). This adaptability has inspired the development of frameworks that integrate COBIT principles to address emerging challenges like big data management and privacy concerns (ISACA, 2013).

The framework's performance measurement criteria help organizations assess cybersecurity maturity. COBIT enables evaluations of IT governance capabilities, identifies gaps, and offers recommendations for improvement (Purnama et al., 2020). Its maturity models are compatible with other standards like NIST CSF and PCI DSS, providing an integrated approach to assessing cybersecurity readiness (Sulistyowati et al., 2020). This structured assessment process equips businesses to enhance IT governance while staying resilient against evolving cyber threats.

COBIT's versatility is further demonstrated through its integration with other frameworks, such as ISO 27001 and NIST CSF. Mapping COBIT processes to ISO standards enhances compatibility while embedding COBIT principles within the NIST

Cybersecurity Framework creates synergies in addressing shared objectives (Sheikhpour & Modiri, 2012; ISACA, 2014). Despite differences in scope and terminology, innovative methodologies like Enterprise Architecture metamodels streamline the assessment and implementation of these frameworks (Almeida et al., 2018).

For smaller organizations, COBIT adapts to resource constraints through tools like COBIT Quickstart, which offers baseline IT governance controls (Devos, 2007). The COBIT 2019 Design Toolkit further supports small and medium enterprises (SMEs) by aligning business and IT strategies, although some usability challenges persist (Amore et al., 2023). While often seen as complex for SMEs, COBIT's tailored applications prove its potential to provide valuable governance solutions for smaller entities (Mijnhardt et al., 2016).

Emerging technologies like IoT and cloud computing pose unique challenges, and COBIT addresses these through structured risk management strategies. For IoT, COBIT guides the development of security measures to safeguard data privacy and protection (Latifi & Zarrabi, 2017; Henriques et al., 2021). Cloud computing, offers foundational governance principles, though additional refinements are necessary to address all emerging risks (Bounagui et al., 2016). The convergence of IoT and cloud computing, referred to as the Cloud of Things (CoT), underscores COBIT's importance in managing security and privacy concerns in these evolving paradigms.

COBIT offers a comprehensive model for IT governance and cybersecurity, equipping organizations to manage risks, ensure compliance, and align IT initiatives with strategic goals. Its adaptability to various contexts, from small enterprises to large-scale implementations, ensures its continued relevance in today's dynamic technological environment. Integration with other methodologies and emphasis on continuous

improvement, COBIT remains an indispensable tool for organizations striving to strengthen their cybersecurity posture.

## **2.6 Risk Management Framework (RMF)**

The Risk Management Framework (RMF) is a systematic approach to managing information system security risks within organizations. It has six steps: security categorization, control selection, control implementation, control assessment, system authorization, and continuous monitoring. These steps enable near real-time risk management and foster continuous system authorization by embedding security measures directly into enterprise workflows and system development life cycles.

The RMF stands out for its adaptability across various organizational environments. Although originally developed for federal systems, it has proven to be an effective tool for managing the complexities of modern cloud computing environments. By concentrating on risk identification, assessment, mitigation, and continuous monitoring, the RMF enables organizations to comply with regulations while addressing evolving security challenges (Arogundade, 2023). This versatility extends its value to private companies and small businesses, making it useful far beyond its initial federal applications (Dana-Marie Thomas et al., 2022).

A core strength of the RMF is its focus on integrating security into the system development life cycle (SDLC). By addressing security requirements early in the development process, organizations can ensure that systems are better prepared to withstand threats before they are deployed. This proactive approach enhances decision-making for senior leaders, enabling them to make informed and cost-effective choices that support their organizational goals while staying compliant with frameworks like FISMA (Ross et al., 2004). Additionally, continuous monitoring ensures that systems remain

secure over time, fostering accountability and linking individual controls to broader organizational risk management strategies (Unuakhalu & Garikapati, 2014).

The RMF also excels in tailoring security measures through its categorization process. By assessing the potential impact of breaches on confidentiality, integrity, and availability, organizations can apply security controls in a precise and effective manner, avoiding both over-engineering and under-engineering solutions (Witzke, 2015). Furthermore, the RMF's flexibility allows for enhancements such as incorporating role-based access control (RBAC), which can simplify the management of larger, more complex systems (Sandhu et al., 1996).

When compared to other frameworks like NIST CSF and ISO 27001, the RMF offers a distinct advantage. While NIST CSF emphasizes cybersecurity readiness and ISO 27001 focuses on compliance, the RMF uniquely integrates privacy and security controls into everyday workflows, providing a structured and dynamic approach to risk management. This focus supports continuous improvement in an organization's overall security posture (Alghamdi, 2023; Almuhammadi & Alsaleh, 2017).

Despite its roots in federal applications, the RMF is well-suited for small businesses looking to enhance their cybersecurity practices. By applying tailored RMF principles, such as the Distributed Energy Resource Risk Manager (DER-RM), even smaller organizations can implement scalable and cost-effective security solutions (Dana-Marie Thomas et al., 2022). This makes the RMF a practical choice for fostering resilience in a variety of operational settings.

In conclusion, the RMF's structured, flexible, and adaptable design establishes it as a cornerstone of cybersecurity risk management. By integrating security into daily workflows, prioritizing continuous monitoring, and aligning with compliance standards, the RMF provides a solid foundation for managing information system risks. Beyond

supporting existing frameworks, it offers unique insights into aligning technical controls with organizational priorities, ensuring sustained security and long-term success in a constantly shifting threat landscape.

## **2.7 ISO/IEC 27005**

Information security is complex, yet essential. Organizations worldwide rely on ISO/IEC 27005 to navigate these challenges effectively. This framework seamlessly integrates with ISO 27001, offering practical guidance for risk management (Bahtit & Regragui, 2013; Cerqueira Junior & Arima, 2023). Many businesses find success in implementing ISO 27001 through this systematic control approach (Syopiansyah et al., 2020).

The journey begins by understanding unique organizational contexts before moving through the identification, analysis, and evaluation phases. Traditional qualitative methods remain popular, though sophisticated approaches using fuzzy logic and multi-criteria analysis have emerged (Shameli-Sendi et al., 2012). Recent developments introduced UML modeling techniques, expanding decision-making capabilities (Bahtit & Regragui, 2013).

The synergy between ISO/IEC 27005 and ISO/IEC 27001 creates remarkable results (Wahlgren et al., 2013). While one addresses risk specifics, the other builds comprehensive security foundations. Together, they form an unbreakable chain protecting information assets and ensuring regulatory compliance (Cerqueira Junior & Arima, 2023).

Reality presents various obstacles during implementation. Technical complexities intertwine with regulatory demands and operational hurdles. Human elements, particularly knowledge gaps and awareness issues, require attention (Sussy et al., 2015). Success stories emphasize comprehensive training programs and transparent communication channels



(Werlinger et al., 2009). Flexibility remains key, allowing customization based on unique organizational requirements.

Vigilance through continuous monitoring shapes long-term success. Regular reviews ensure risk management strategies evolve with emerging threats (Hamir & Sum, 2021). Strategic integration of security measures aligns perfectly with broader business objectives (Barafort et al., 2017).

Beyond technical requirements lies strategic evolution. ISO/IEC 27005 transforms organizational security postures through methodical approaches and adaptable frameworks. Small enterprises and global corporations alike discover pathways to confident risk management. Every organization charts its course while maintaining an unwavering focus on information security excellence.

## **2.8 NIST Privacy Framework**

The landscape of privacy risk management finds its cornerstone in the NIST Cybersecurity Framework. This tool shapes how federal systems and healthcare organizations protect sensitive information, bringing together engineering principles and risk modeling to strengthen privacy understanding (Brooks et al., 2017). Working alongside the NIST Cybersecurity Framework and Risk Management Framework, it weaves privacy into broader risk strategies (Williams et al., 2020). Healthcare systems particularly benefit, as privacy becomes fundamental to patient safety and smooth operations (Williams et al., 2020).

Yet challenges persist beneath the surface. While joining forces with cybersecurity methods, the framework struggles with modern privacy threats, particularly those involving inference-based risks where sensitive details emerge from seemingly harmless

data (Landis & Kroll, 2024). These gaps point toward needed updates in risk controls and policy alignment.

At its heart lies the Core, introducing essential privacy engineering ideas and risk management vocabulary (Brooks et al., 2017). This proves invaluable during crises when privacy might otherwise take a backseat to security concerns. Organizations achieve both resilience and privacy protection by weaving these principles into their systems and emergency plans (Hiller & Russell, 2017).

The Profile feature lets organizations shape privacy strategies around their unique circumstances. While tools like Baseline Tailor make implementation smoother (Lubell, 2016), recent studies show room for growth, especially regarding inference-based privacy threats (Landis & Kroll, 2024).

Through Implementation Tiers, organizations gauge their privacy and security practices effectively. Research suggests adding economic frameworks like the Gordon-Loeb Model could optimize resource allocation (Gordon et al., 2020). Scholars have proposed enhancing the framework's connection to the NIST Cybersecurity Framework through maturity assessments (Almuhammadi & Alsaleh, 2017).

Smaller enterprises wrestling with limited resources often find the framework's abstract concepts challenging to implement, despite its solid foundation. Fresh research points toward evolving solutions that blend machine learning with social and technical approaches to meet these unique business needs (Al-Dosari & Fetais, 2023). Making the framework more practical and scalable for small businesses would significantly boost its real-world value.

Looking beyond technical aspects, this framework serves as a crucial bridge to regulatory compliance with GDPR, CCPA, and similar privacy laws. It helps organizations thread the needle between legal obligations and day-to-day operations, keeping efficiency

and trust intact (Ghorashi et al., 2023). Yet work remains, particularly around data minimization and purpose limitations. As our digital landscape shifts, the framework must keep pace to maintain strong privacy safeguards (Finck & Biega, 2021).

Trust blooms naturally when privacy becomes part of system architecture, especially during critical moments. Organizations embedding both security and privacy demonstrate their genuine commitment to protecting user information. This thoughtful approach cultivates lasting trust and establishes privacy as a cornerstone of organizational identity (Hiller & Russell, 2017).

## **2.9 Comparing and Integrating Frameworks**

Cross-referencing these approaches streamlines compliance while meeting both regulatory needs and internal risk targets (Wang et al., 2024). Manufacturing spaces using Industry 4.0 and 5.0 particularly benefit when NIST CSF joins forces with ISO 27001 (Barraza de la Paz et al., 2023).

Each framework brings its flavor to the table. Risk-focused ones like ISO 27005 and RMF bend to match specific organizational needs, while compliance-driven frameworks like ISO 27001 follow strict control sets (Roy, 2020; Wahlgren et al., 2013). This distinction highlights the importance of tailoring framework adoption to an organization's size. Smaller players often shine using mixed approaches that balance security and privacy within tight budgets (Chandna & Tiwari, 2021).

The industry, regulations, and risk appetite shape which frameworks fit best. While powerhouses like NIST SP 800-53 and ISO/IEC 27001 pack comprehensive protection, their complexity can overwhelm smaller shops (Kurii & Opinsky, 2022). For such organizations, adopting a modular approach allows for gradual implementation and maturity development. Some grow into it slowly, piece by piece. Meanwhile, cutting-edge

options like MAGERIT and the fresh ISO/IEC 27001:2022 tackle today's digital risks head-on (Barraza de la Paz et al., 2023).

Juggling multiple frameworks is not always smooth sailing. Tools clash, security gaps pop up, and efficiency takes a hit. Organizations often stumble trying to merge different approaches, especially when compliance bumps heads with risk management (Bahuguna et al., 2018; Cater-Steel et al., 2006). While combining tools might help, watch out for getting stuck with vendors or messy transitions (Ajish, 2024).

Cybersecurity and privacy frameworks go hand in hand; they show why joining forces matters. NIST's Cybersecurity and Privacy Frameworks team up for unified risk handling (Barrett et al., 2020). Healthcare especially needs this harmony to keep security and privacy in sync (Williams et al., 2020).

Tech keeps pushing boundaries. AI and machine learning now hunt threats, while blockchain promises tougher infrastructure (Sontan Adewale Daniel & Samuel Segun Victor, 2024; Douha Jerbi, 2023). With quantum computing and clever attackers coming, risk strategies must stay sharp (Harshada Umesh Salvi & Supriya Santosh Surve, 2023). Making frameworks work together needs both tech smarts and business sense. Pick your frameworks wisely, blend them carefully, and build security that lasts in our wild digital world.

## **2.10 Gaps in Existing Literature**

Exploring key areas needing attention in cybersecurity research, the literature review points to several crucial gaps that future studies should tackle to build better security frameworks, especially for smaller businesses.

- **Empirical Validation:** we need more real-world proof. While many talk about how well these frameworks work, we're short on actual studies comparing their effectiveness across different types of organizations.
- **Integration Challenges:** The nuts and bolts of putting multiple frameworks together remain tricky. We need deeper dives into practical hurdles like overlapping tools and messy operations, plus solid strategies to overcome these roadblocks.
- **Adaptation for SMBs:** Small and medium businesses need more attention. Sure, there's talk about frameworks for them, but we need concrete studies showing what works and what needs tweaking for smaller players.
- **Dynamic Threat Adaptation:** Keeping up with threats is another challenge. We're light on research about how frameworks can quickly adapt to new dangers, especially with AI, IoT, and blockchain shaking things up.
- **Privacy Risk Alignment:** Privacy risks deserve more spotlight too. While some work connects privacy and security frameworks, we need better tools for managing privacy risks, particularly in data-heavy fields.
- **Framework Comparisons in Specific Industries:** Industry-specific comparisons could use work. We'd benefit from detailed studies showing how different frameworks perform in healthcare, finance, and critical infrastructure.
- **Quantitative Assessment Models:** organizations need better ways to measure costs and benefits when adopting various frameworks, especially when using several at once.

- Cultural and Organizational Resistance: Cultural resistance is worth exploring. We should study what stops organizations from embracing these frameworks and how to overcome pushback, especially globally.
- Ethical and Legal Considerations: Legal and ethical angles need attention. More analysis of how laws and ethics affect framework implementation would help, particularly with international rules.
- Post-Implementation Impact: we need long-term impact studies. How do these frameworks hold up over time as threats and technology evolve?

Looking at the big picture, this review covers how various frameworks like NIST CSF, ISO/IEC 27001, COBIT, and CIS Controls help manage digital risks. Each brings something unique to the table, but gaps remain - especially around proof they work, integration challenges, and making them work for smaller businesses.

The field keeps changing as technology races forward and new threats emerge. Small businesses particularly struggle, often lacking the resources and expertise to use these frameworks effectively. We need fresh research to understand what holds these businesses back and what helps them succeed.

Next up, we'll dive into research methods, laying out how we'll tackle these gaps. We're focusing especially on small business challenges with current frameworks. Through careful study, we aim to offer practical insights and recommendations, making cybersecurity frameworks more accessible to all organizations, and helping them stay secure in our complex digital world.

## CHAPTER III: METHODOLOGY

This chapter delineates our methodical approach to studying cybersecurity in small businesses, with an emphasis on developing a tailored framework that is both accessible and sustainable. By employing a mixed-methods design, we aim to garner comprehensive insights from both quantitative data and qualitative experiences, enabling us to formulate practical recommendations that can enhance cybersecurity practices within resource-constrained environments. This chapter not only outlines the research design and methodological rationale but also details the iterative processes involving surveys, interventions, and consultations, all geared towards generating actionable insights that inform the creation of a minimalistic cybersecurity framework suitable for small businesses.

### **3.1 Research Design**

The study can be classified as descriptive research as it sheds light on the landscape of existing cybersecurity practices and highlights their awareness among small businesses. It also shares elements of exploratory research as it Investigates which cyber security frameworks can be used by small businesses considering the resource constraints and limited capabilities. The study features a multi-phase approach where data is collected quantitatively as well as qualitatively. The analysis techniques are descriptive statistics as well as content and thematic analysis. The study also consists of a framework development where grounded theory principles are used and can be considered applied research. All these features make this study a fit closest to the mixed-method approach.

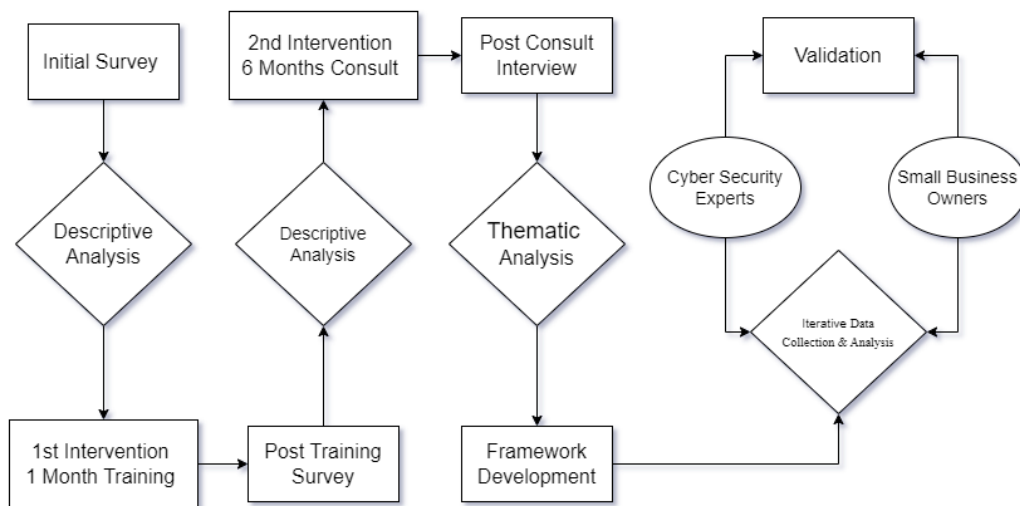


Figure 3a: Illustration of Research Design Phases, Source: (Original Work)

### 3.2 Rationale for Choosing Mixed-Methods Approach

Mixed methods research represents a sophisticated methodological approach that strategically integrates both quantitative and qualitative research techniques to achieve a comprehensive understanding of complex research inquiries (Turner et al., 2017; Caruth, 2013). Primarily, this particular cohesive approach has become increasingly famous among researchers and scholars, as it enables the exploration of intricate phenomena that might have not captured their full potential when relying solely on either quantitative or qualitative methodologies. By synthesizing these diverse methodologies, mixed methods research provides nuanced insights that can lead to more informed conclusions (Caruth, 2013). There are several distinct designs, including sequential, concurrent, multiphase, and multilevel approaches in mixed method methodology. This variety offers researchers a sense of empowerment, allowing them to choose the design that best suits their research questions and objectives (Almeida, 2018). Sequential designs typically involve the collection and analysis of data in phases, where one phase of research informs the next.



While this method can be linear relatively, generally, it demands an investment of time and effort to complete each phase. In contrast, concurrent designs allow researchers to collect qualitative and quantitative data simultaneously, expediting the overall data collection process. Nevertheless, this method may give rise to unseen challenges when integrating and synthesizing the results from these two distinct data types. By being aware of these challenges, researchers can better prepare for the analytical process (Almeida, 2018). The successful execution of rigorous mixed methods studies necessitates that researchers possess a high level of proficiency in both quantitative and qualitative research techniques (Caruth, 2013). This dual competency is a dire requirement and a testament to the competence of researchers in ensuring that the methodologies used are appropriately matched to the specific research questions and that the data collected is effectively integrated. In addition, integrative mixed methods designs that combine confirmatory findings derived from quantitative analyses with rich explanatory insights from qualitative data can significantly bolster the research's overall robustness and scientific integrity (Castro et al., 2010).

### **3.3 Initial Survey and Descriptives Analysis**

The data collection processes started with a survey questionnaire (refer to Appendix A) to understand cybersecurity awareness and readiness among small business owners. The survey was designed to capture a wide range of data, including business demographics, awareness of cybersecurity risks, current practices, knowledge of established cybersecurity frameworks, and willingness to invest in cybersecurity improvements. The questions were structured into six sections, each addressing a specific aspect of cybersecurity, such as demographic information, prior incidents, implemented measures, and barriers to adopting frameworks. A stratified random sampling technique was adopted to ensure comprehensive

representation across industry sectors. The strata were precisely defined based on industry type, carefully considering the proportion of firms in each one of them. A targeted sample size of 300 small businesses ensured the research's robustness and practicality.

The survey underwent a pretesting phase when a small sample of businesses was used to improve the questions and verify that they were clear. The surveys were distributed physically to the designated sample. Reminders were sent to increase the response rates. A window of eight weeks was offered to provide sufficient time for collecting answers. Descriptive statistics was utilized to summarise survey questionnaire data, offering valuable insights into the prevalence of cybersecurity practices and incidents among small businesses. Minitab was utilized for data analysis, ensuring robust and precise computation of results.

### **3.4 First Intervention by Researcher – 1 Month Training**

The initial survey resulted in the identification of core issues with a lack of awareness of cybersecurity best practices and the capability to implement existing cybersecurity frameworks. To resolve this, an Intervention was required by the researcher where small business owners were educated and trained on NIST CSF, ISO/IEC 27001, and NIST RMF. The training sessions focused on simplifying these frameworks to make them accessible and relevant to small business operations. Workshops were conducted both online and in person. Case studies and real-world examples were used to demonstrate the impact of cybersecurity breaches and the value of adopting structured frameworks like NIST CSF and ISO/IEC 27001. Additionally, the training highlighted cost-effective strategies for resource-constrained businesses, including leveraging free tools, developing basic cybersecurity policies, and fostering a culture of security awareness among employees. Feedback from participants was collected to evaluate the effectiveness of the

intervention and to identify areas requiring further support or clarification. This intervention laid the foundation for assessing whether increased knowledge and practical guidance could lead to improved cybersecurity practices in small businesses.

### **3.5 Post Training Survey**

Following the first intervention by the researcher, a post-training survey (refer to Appendix B) was conducted to evaluate the impact of the intervention and gather feedback from participants. The survey focused on assessing the participants' understanding of the frameworks, the progress made in implementing them, the challenges encountered, and the perceived business impact. Structured into five sections, the survey captured qualitative and quantitative data to evaluate both the effectiveness of the training and the readiness of small businesses to adopt these cybersecurity frameworks.

The first section measured participants' understanding and confidence levels for each framework, providing insights into the knowledge gained during the training. The second section focused on implementation progress, identifying which frameworks had been adopted and the specific steps completed, such as risk assessments, security policy development, or incident response planning. Participants who had not started implementation provided reasons, offering valuable context for barriers such as time constraints or cost concerns. The third section explored challenges faced by businesses, highlighting common difficulties such as limited budgets, technical expertise gaps, and integration issues with existing systems. It also solicited suggestions on the types of support that could address these barriers, such as additional training, expert consultations, or more affordable tools. The fourth section assessed participants' perspectives on the business impact of the frameworks and their plans, including the likelihood of full implementation within six months. Finally, the survey included open-ended questions in Section 5,

allowing participants to provide specific expectations, outcomes, or requests for further support.

### **3.6 Second Intervention by Researcher – 6 Months Consultations**

Building on the findings of the post-training survey, the researcher initiated a free 6-month consultation campaign. The goal was to provide expert guidance tailored to the unique operational needs of each business, enabling them to effectively implement and sustain cybersecurity measures. The following objectives were pre-determined:

1. **Addressing Technical Expertise Gaps:** Provide businesses with expert support to overcome challenges related to understanding and implementing technical aspects of the NIST CSF.
2. **Customized Framework Implementation:** Tailor the application of NIST CSF to the specific size, resources, and operational constraints of each business.
3. **Building Confidence and Capacity:** Empower business owners and employees by working alongside them to develop practical, sustainable cybersecurity practices.
4. **Overcoming Resource Barriers:** Identify and implement cost-effective solutions to mitigate financial constraints and resource limitations.

Small businesses that participated in the initial training and post-training survey were invited to join the consultation phase. A total of 25 businesses were selected, representing diverse industries to ensure broad applicability of the findings. Each participating business underwent an initial consultation to assess its current cybersecurity posture, specific challenges, and implementation progress. Based on the initial assessments, customized action plans were developed for each business. These plans outlined step-by-step procedures for implementing the NIST CSF, considering the business's unique constraints

and requirements. Businesses were assigned dedicated consultation slots where they were provided one-on-one guidance.

### **3.7 Post-Consultation Interview & Thematic Analysis**

The post-consultation interview (refer to Appendix C) was conducted to evaluate the effectiveness of the six-month consultation process and to gain qualitative insights into the experiences of small businesses in implementing the NIST CSF. This phase was essential to assess the outcomes of the expert-driven intervention and to identify any remaining barriers or areas for improvement. The objectives were as follows:

1. To evaluate the progress made by businesses in implementing the NIST CSF with expert guidance.
2. To identify challenges that persisted during or after the consultation phase.
3. To capture the perceived benefits and business impact of implementing the NIST CSF.
4. To collect feedback on the consultation process and identify potential improvements.
5. To inform future research and practical recommendations for supporting small businesses in enhancing their cybersecurity practices.

The participants for the interviews were the same 25 small businesses that engaged in the six-month consultation phase. The interviews were semi-structured, ensuring consistency across participants while allowing flexibility to explore individual experiences in greater depth. The interview guide included broad thematic areas such as challenges during implementation, impact, and benefits of the NIST CSF, evaluation of the consultation process, and future outlook. The interviews were conducted virtually using Google Meet, based on participant preference, and lasted approximately 30–45 minutes each. Informed

consent was obtained from all participants, ensuring ethical compliance. Interviews were recorded with permission, and transcribed to ensure accuracy and thoroughness.

A thematic analysis approach was used to identify recurring patterns, themes, and insights from the interview data. Responses were categorized into key themes, such as challenges, perceived benefits, consultation feedback, and plans, to provide a structured understanding of participant experiences.

### **3.8 Framework Development Using Grounded Theory**

The preceding phase of the research identified significant challenges small businesses face. It was determined that frameworks are humongous and complex for small businesses. Therefore, it calls for a more streamlined and practical approach to cybersecurity that organizations with limited resources and expertise can readily adopt, scale, and maintain.

Based on these findings, a minimalistic cyber security framework (MCSF) was devised, utilizing a product development methodology inspired by grounded theory. This theoretical framework was chosen due to its innate appropriateness for creating a practical framework directly informed by real-world insights, particularly derived from the robust qualitative data gathered through interviews with cyber security experts. Rooted in the thematic analysis were the multiple challenges small businesses face when adopting cybersecurity frameworks. These issues included:

- The lack of internal expertise is essential for effectively implementing and managing cybersecurity protocols.
- Existing misalignment between cybersecurity initiatives and business priorities, with a predominant focus on growth rather than security.

- The complexity of existing cybersecurity frameworks can oftentimes be a barrier to practical application.
- The substantial costs and requisite resource allocations needed for comprehensive cybersecurity implementation.
- An inability to retain sustainable cybersecurity practices over the long term without reliance on external support.

Inevitably, these insights identified the challenges but also led to a promising solution. This novel approach simplified cybersecurity into essential and manageable components, illuminating a beacon of hope for better integration within small business operations. In alignment with the ethos of grounded theory, the development of the framework was conducted through an iterative process, compiling feedback loops at each stage. Expert opinions played a critical role in the development of the framework, ensuring that it effectively addressed the identified challenges. Each iteration was modified to enhance both practicality and relevance.

### **3.9 Validation Interview**

Building on the foundation of the earlier consultations and the development of the framework, a final assessment was conducted through an interview (refer Appendix I) with the small businesses that had participated in the consultation and framework implementation process (refer. These interviews aimed to evaluate the practical effectiveness of the newly developed framework and to gather feedback on its usability, alignment with business needs, and overall impact on cybersecurity practices.

The interview process was structured around six core themes, derived from the interview guide, and provided valuable qualitative insights into how small businesses perceived and implemented the proposed framework.

### **3.10 Ethical Considerations:**

Informed consent was obtained from all participants from the survey, interviews, and intervention phases. They were fully aware of the purpose of the research, their rights, and how their data was to be used.

Upholding the confidentiality and anonymity of participants and their data is crucial, Hence all PII and other sensitive information was protected and not disclosed in the results. It is available on requests made explicitly to the researcher or SSBM to be evaluated on an individual basis.

All the data collected and analyzed in the research was securely stored in a biometric-secured flash drive with disk-level encryption and other access controls to prevent unauthorized access and breaches. The drive was then stored in an isolated safe which will be retained for a period of 8 years from the date of publishing this study.

The methodology outlined in this chapter serves as the foundation for developing a cybersecurity framework tailored to the unique needs of small businesses. By employing a mixed-methods approach, integrating both quantitative and qualitative data, we ensure a comprehensive examination of the current cybersecurity landscape. The deliberate sequence of surveys, interventions, consultations, and thematic analyses provides a robust mechanism to identify and address the core issues small businesses face in adopting existing frameworks. This methodological rigor not only enhances the validity of our findings but also ensures that the recommendations and frameworks we propose are informed, pragmatic, and ready to be scaled across diverse small business contexts. The subsequent chapters will delve into the findings and analysis arising from this well-



structured methodology, paving the way for actionable solutions that empower small businesses in their cybersecurity endeavors.

## CHAPTER IV: RESULTS

In this chapter, we will delve into the findings from our comprehensive study on cybersecurity among small businesses. Through surveys, training programs, consultant interventions, and interviews, we systematically explore the gap between awareness and practical application of cybersecurity measures. Our objective is to uncover the prevalent understanding of cybersecurity risks, the barriers faced in adopting robust frameworks, and the readiness of small businesses to invest in strengthening their defenses. This chapter meticulously presents the results of several approaches designed to enhance cybersecurity resilience, offering valuable insights into the specific needs and challenges encountered by small businesses.

### **4.1 Cybersecurity Awareness Among Small Businesses**

The research utilized a survey in which 300 small businesses from various industries participated. The results disclose critical perceptions of small business owners' cybersecurity awareness, preparedness, and potential.

Among the participating respondents, 67% identified their awareness of cybersecurity risks as "moderate" or higher, while only 25% rated their understanding as "high" or "very high," emphasizing tremendous lacuna in comprehensive knowledge. Alarmingly, 30% of businesses reported experiencing a cybersecurity incident, with data breaches (45%) and phishing attacks (30%) being the predominant threats.

Although 60% of respondents have adopted fundamental cybersecurity protocols, such as antivirus solutions, only 20% have implemented more sophisticated measures like multi-factor authentication (MFA) or consistent employee training. These divergences depict recognition of cybersecurity needs; unfortunately, the execution tends to be superficial. Moreover, only 12% conduct annual reviews of their cybersecurity posture.

Conversely, a significant 35% reevaluate only post-incident, underscoring a reactive stance instead of a proactive approach to risk management.

The survey also highlights that only 45% of participants are aware of formal cybersecurity frameworks, with the NIST Cybersecurity Framework and CIS Controls being the most generally recognized. Nevertheless, only 18% of respondents have successfully implemented the framework.

Cost (35%), lack of technical knowledge (40%), and low-risk perception (25%) stand as the biggest obstacles to self-regulation. This has pointed out a significant potential for enhancing the availability of such frameworks to the micro-enterprises that may, with any luck, help strengthen their cyber security. The readiness of this majority to invest funds is an expression of their active posture as regards cyber security which makes a lot of sense, especially within the context of rapidly growing threat vectors such as ransomware and phishing scams. For instance, a good number of the respondents were unwilling to indicate ways in which they would practically seek to reduce these risks.

Interestingly, 58% of firms recognized the positive effects of using a cybersecurity framework to mitigate major risks such as slow response time and enhanced threat awareness arguing that further training and clarification could have significant positive effects on compliance.

From what the respondents indicated, their level of sophistication was moderate when it came to knowing much about cybersecurity regulations but their depth of understanding of most practices was relatively shallow. Existing challenges such as cost and lack of skills make a compelling case for the need for affordable and simple usage of cyber security tools.

Only 30% of respondents rated their confidence in executing a cybersecurity framework as moderate or higher. Despite this, 65% expressed a willingness to invest in

cybersecurity initiatives, with half committed to allocating a budget towards employee training and 40% considering hiring external professionals.

#### **4.2 Small Business of Cybersecurity Frameworks After Training**

After a month of training on the NIST Cybersecurity Framework (CSF), ISO/IEC 27001, and the NIST Risk Management Framework (RMF), the results of a subsequent survey revealed substantial challenges small businesses face in comprehensively understanding and implementing these frameworks. Though the respondents underwent well-planned and structured training sessions, they found implementing and integrating these frameworks into their ongoing business tricky and cumbersome.

While the initial survey showed a baseline, there was a marginal improvement in understanding following the month of training. Only 35% of respondents rated their understanding and comprehension of the NIST CSF as "moderate" or better, and for ISO/IEC 27001, this percentage was quite lower at 25%. Nevertheless, this also means that there is a significant potential for improvement. Only 20% of participants reported having a "moderate" or better understanding of the NIST RMF. However, with the help of continued support and training, there can be a marked rise in percentage. A significant portion, 45% of respondents, indicated "basic understanding" or "no understanding" of the frameworks. This points out that while awareness of the frameworks has increased, thorough comprehension remains limited but not unattainable.

The confidence level in implementing the existing cybersecurity frameworks is oddly low across various organizations. It was observed that only 28% of businesses reported feeling "moderately confident" or better regarding their capability to implement the NIST Cybersecurity Framework (CSF). Even fewer, at 20%, expressed confidence in applying ISO/IEC 27001.

On the other end of the spectrum, the NIST Risk Management Framework RMF saw the lowest levels of confidence in the eyes of participants, with only 15% saying they could apply the framework effectively. This in itself exacerbates the large chasm experienced between possessed information and the ability to perform task completion.

Despite undergoing a month-long training program, only 20% of businesses registered that they had initiated the implementation of the NIST CSF, with an even smaller percentage (10%) recording any progress on ISO/IEC 27001 or the NIST RMF. Among those that had initiated implementation, most had only undertaken preliminary actions, such as performing basic risk assessments or identifying cybersecurity vulnerabilities. No respondents reported accomplishing full implementation of any of the frameworks.

The main barriers reported for the launch or continuation of implementation efforts are a lack of technical know-how 40%, insufficient funds 35%, and uncertainty about what would happen next 30%. It means this industry needs cooperation and mutual resource sharing.

After the conclusion, prominent challenges that appeared during the training continued to persist. A considerable proportion of businesses, specifically 50%, described it as tedious to comprehend the technical requirements of the frameworks, while 45% identified limited internal expertise as a significant deadlock. Also, 40% of business owners reported that budgeting is one of the significant limits that a business faces. This highlights how, in practice, even small businesses will not always be able to afford the cybersecurity they need across the company, making a great appreciation of the need for assistance in such a place important. Further questioning the potential advantages of embracing these models, a meager 40% agreed or strongly agreed with the statement, whereas the preliminary survey indicated. This decline is an increase in skepticism or dissatisfaction as organizations face the intricacies involved in the implementation process.

In addition, only 25% of respondents reported an intention to fully implement a cybersecurity framework in the next six months, which calls for reassessment and possibly changes in the training approach.

The findings of this survey reveal a significant gap in cybersecurity practices. While the month-long training sessions have successfully improved awareness and theoretical knowledge of cybersecurity frameworks, the practical application of this knowledge continues to be challenging for numerous small businesses. The dearth of technical expertise, insufficient resources, and a lack of confidence in implementing these frameworks continue to leave small businesses vulnerable to cyber threats despite their intent to reinforce security measures.

This suggests that intervening cybersecurity specialists should be incorporated into future research for purposes of assisting businesses in the implementation process. Also, as consultants, these specialists can work together with each business to face their specific needs and customize the frameworks to suit the requirements of operations. After this phase of expert-guided implementation, a survey can be conducted to gauge whether businesses can productively integrate and sustain these essential cybersecurity measures.

### **4.3 Thematic Analysis of Post-Consultation Interviews**

The transition from the training phase to the hands-on support stage was next where the preceding phase accrued valuable insights into the real-world challenges that small businesses face in adopting cybersecurity frameworks, thereby providing a pathway toward more sustainable and long-term cybersecurity resilience.

The thematic analysis of interview responses unearthed several key themes, implying that the NIST Cybersecurity Framework (CSF) and comparable frameworks, such as ISO/IEC 27001, may be extremely complicated and resource-intensive for small

businesses, particularly startups. Regardless of engaging in expert consultation over three months, feedback from small business owners suggests that even the simplified versions of these frameworks—such as the NIST CSF Small Business Implementation Guide and various community profiles—could not accommodate their distinct needs. This calls out the crucial role of cybersecurity professionals, small business owners, and policymakers in finding tailored solutions to these challenges. Below is the delineation of the major themes identified during the interviews.

#### **4.3.1 Overwhelming Complexity of Frameworks**

Several small business owners proclaimed that the exhaustive nature of the NIST CSF was arduous to comprehend and implement, despite professional guidance. The language and structure of the framework were anticipated as overly technical for their organizational capacities. One business owner shared, "Despite collaborating with the consultant, I am still not able to grasp all the terminology within the framework. It seems to be orientated toward large organizations rather than small entities of our size."

Insight: This suggests that further work should focus on interventions that involve the participation of cybersecurity professionals in the execution stage to support organizations. These professionals act as consultants and can assist with the particular problems of each firm and customize the frameworks to fit their needs. The NIST Cyber Security Framework (CSF) consists of five core concepts Identify, Protect, Detect, Respond, and Recover—alongside intricate subcategories that often bewilder small business proprietors. Most small business owners are often overwhelmed with the complexities and requirements of the five functions and their subcategories. The reality of having to juggle running a business while trying to understand and implement such a broad framework is unfortunately something this population can understand all too well.

### **4.3.2 Insufficient Resources and Know-How**

The lack of funds and the specialized staff are characteristic of small business enterprises. A common complaint is the seemingly low internal capacity, in terms of human resources and financial budgets, available for the adoption and management of such a wide-ranging framework. More so, even when there are external consulting efforts, most firms are unable to invest more time and people to implement the recommended measures. One startup owner succinctly noted, "Frankly, we lack a dedicated IT team, let alone a cybersecurity expert. Balancing this with our other operational demands is unmanageable." Small businesses, particularly startups, generally engage with lean teams that prioritize growth and core operational functions.

Insight: Often, the specialized expertise needed for the implementation and maintenance of the NIST Cybersecurity Framework (CSF) or ISO 27001 is above and beyond the internal capabilities of these organizations. Henceforth, they become reliant on costly external consultants for long-term sustainability.

### **4.3.3 Misalignment with Startup Priorities**

Startups have cited the NIST CSF as a misalignment with their immediate business objectives, as their priority is rapid growth and market penetration rather than comprehensive security frameworks. The requisite time and resources to implement such a framework are seen as distractions from their principal goals. One participant stated, "Currently, our focus is on developing products and acquiring customers. Allocating weeks for implementation of a security framework does not make sense and does not match with our current priorities."

Insight: Generally, startups work under resource constraints and an accelerated sense of urgency. These are common challenges that many startups encounter. Many of



these organizations note that adopting frameworks such as the NIST CSF or ISO 27001 is a consideration for the future rather than an immediate necessity, particularly in the absence of significant cybersecurity incidents.

#### **4.3.4 Limited Applicability**

The NIST Cybersecurity Framework (CSF) Small Business Implementation Guide and associated community profiles designed to simplify the implementation process have been observed as overly complex and insufficiently tailored to the realities encountered by distinct small businesses. Many respondents noted that these guides tended to be too ambiguous and did not adequately address the specific needs of various industries. A small business owner observed, "The Small Business Guide provided a foundational understanding; nevertheless, when it came to implementation, more support was required than what the guide delivered."

Insight: Although these materials target structural inequalities among large organizations and small businesses, most of the respondents reported that there was a shortage of practical industry examples or simple steps that would be easy to implement for businesses with few cybersecurity skills

#### **4.3.5 Cybersecurity as Non-Essential Function**

Many businesses have perceived cybersecurity as a secondary priority until they accomplish a certain growth milestone. For many, the anticipated risks of cyberattacks do not exceed the innate pressures to expand and acquire new customers. One participant expressed, "We have not experienced any security issues so far, and it seems to be a future probable concern that can be tackled later once we are more established."

Insight: This mindset illustrates that numerous small enterprises adopt a reactive instead of a proactive approach to cybersecurity. Given the lack of experience of a cyberattack, there is limited incentive to allocate significant time and resources to frameworks such as the NIST Cybersecurity Framework, mainly when other business priorities take precedence.

#### **4.3.6 High Cost of Full Implementation**

A recurring issue relates to the considerable financial investment required to implement and maintain cybersecurity frameworks. Investing in cybersecurity measures outside basic protocols for small enterprises, and especially startups, usually requires cutting back on the allocated funds for basic product or marketing activities. One of the business owners raised this issue: “We hardly have enough budget for marketing, let alone for a full-blown cyber security program. It simply does not constitute a feasible financial option for us at this time.”

Insight: Various small businesses sense the financial implications of adopting a framework such as the NIST Cybersecurity Framework—whether through the recruitment of specialized personnel, acquisition of software, or consulting fees—as prohibitive. This high cost often results in hesitation about committing to ongoing expenditures, even when engaging external consultants.

#### **4.3.7 Temporary vs. Sustainable Security Practices**

Numerous small business owners explicitly expressed concerns that, though they could achieve progress with the assistance of a consultant, there was a deficit in the internal capacity to sustain the framework once the consultation period concluded. As a result, they worried that their efforts would not remain viable in the long term. One owner expressed,

"We successfully commenced the process with the consultant's assistance, but I am unsure how we will maintain this momentum after their departure. We do not possess the manpower resource necessary for this."

Insight: This emphasizes the urgent need for more practical and scalable solutions that small businesses can independently maintain. Dependence on external consultants for implementation and management is seen as a transient measure rather than a sustainable long-term strategy.

The thematic analysis of the interviews delineates a definitive conclusion: while frameworks such as the NIST Cybersecurity Framework (CSF), ISO standards, and the NIST Risk Management Framework (RMF) provide substantial value for larger organizations, they often prove exorbitant for small businesses and startups. These entities bear challenges related to complexity, resource limitations, and misaligned priorities. Even resources designed for simplification, such as the NIST CSF Small Business Implementation Guide and community profiles, fail to address their specific needs adequately.

For the majority of small businesses, cybersecurity frameworks remain inaccessible without substantial external assistance, and even with such support, the sustainability of implementation is doubtful. This observation points out a pressing need for a more customized and streamlined approach to cybersecurity that echoes small businesses' unique restraints and priorities. At the outset, it may be judicious to focus on fundamental, scalable security practices that can accommodate the growth of the business rather than imposing comprehensive frameworks. The consequent phase of the research will continue to utilize a hands-on consultancy strategy, reiterating the development of practical, customized solutions that small businesses can implement sustainably.

#### 4.4 Development of a Minimalistic Cyber Security Framework

The new framework was developed to simplify cybersecurity into its most essential components, emphasizing fundamental yet practical practices.



*Figure 4a: Structure of The Minimalistic Cyber Security Framework (MCSF), Source: (Original Work)*

**Basic Protective Measures:** The framework proposed practical, low-cost, and scalable strategies that every small business can adopt without necessitating specialized knowledge. These measures, such as regular software updates, robust password policies, and basic firewall implementations, were designed to be easily implementable, ensuring the framework's feasibility for small businesses.

**Modular Design for Flexibility:** The framework was developed with a modular structure, enabling small businesses to initiate their cybersecurity practices with a fundamental set of guidelines and progressively enhance them as needed. This adaptable design allowed businesses to incrementally advance their cybersecurity measures in alignment with their evolving requirements and available resources.

User-Centric Language and Tools: As highlighted during the interviews, one of the starking loopholes of existing frameworks was the prevalence of technical jargon, which poses comprehension challenges for small businesses. The newly designed framework uses plain language and includes simplified guidelines and checklists, ensuring that it can be easily understood and followed without the necessity for expert cybersecurity knowledge.

Integration with Existing Business Processes: Acknowledging that small businesses prioritize growth and operational efficiency over extensive security frameworks, this methodology was developed to merge with business goals. It seamlessly integrated with existing business processes, ensuring that security practices were harmonized with operational workflows. This approach reassured that cybersecurity becomes a natural extension of daily operations rather than a separate and burdensome task.

#### **4.4.1 Risk Management Strategy Template**

The Risk Management Strategy Template (refer to Appendix D) is not just a theoretical concept but a practical tool that serves as the cornerstone for effectively identifying, evaluating, and mitigating risks within small businesses. Its design provides a clear and practical guide tailored to small businesses, ensuring that they can adopt a proactive and systematic approach to managing risks, even when resources are limited. The template's structure is as follows:

**Introduction:** The Risk Management Strategy commences by establishing a comprehensive understanding of risk management's significance within the context of a small business environment. It underscores the correlation between effective risk management and maintaining a secure operational framework while articulating the organization's unwavering commitment to protecting client, employee, and partner information.

**Objectives:** The objectives outlined in this section are intended to provide a clear direction regarding aligning the risk management strategy with the business's overarching goals. This alignment ensures business continuity, safeguards assets, and adheres to legal and regulatory standards. This framework is designed to assist small businesses in effectively addressing operational, financial, strategic, and cybersecurity risks.

**Risk Management Process:** This section delineates the systematic procedure for managing risks within an organization:

- 1 **Risk Identification:** Small businesses need to identify potential risks regularly. Such risks include cybersecurity threats, legal compliance issues, and operational disruptions.
- 2 **Risk Evaluation:** Tools such as a risk matrix are recommended to assess each identified risk's likelihood and impact. This assessment enables organizations to prioritize risks according to their severity.
- 3 **Risk Mitigation:** The formulation of mitigation strategies is crucial. These strategies may include implementing security controls, employee training programs, or adopting technological solutions to reduce risk exposure.
- 4 **Risk Monitoring:** There is a significant emphasis on the need for continuous monitoring and review through regular audits and assessments. This practice ensures that mitigation efforts remain effective and that the organization can adapt to evolving risks.

**Information Security and Privacy Risk Tolerance:** The template depicts specific sections devoted to managing information security and privacy risks. Regarding information security, it advocates for a low tolerance for breaches, emphasizing the implementation of encryption, access control measures, and regular vulnerability assessments. Concerning privacy, a zero-tolerance stance is adopted, instructing

organizations to minimize personal data collection and enforce privacy measures in compliance with regulations such as the General Data Protection Regulation (GDPR).

**Risk Ownership:** This section elucidates the roles and responsibilities associated with risk management within the organization. It underscores the collective responsibility of all employees, guided by and supported by senior management, to participate actively in risk management initiatives. The formation of a Risk Management Committee or the designation of risk owners is recommended to ensure appropriate oversight and accountability, empowering each individual with the support and guidance of senior management.

**Continuous Improvement:** Embracing the dynamic nature of risks, this strategy underscores the importance of continuously reviewing and updating the framework. This proactive approach ensures that the organization remains responsive to emerging risks, regulatory modifications, and operational advancements and keeps the team motivated and engaged in sustaining resilience.

#### **4.4.2 Asset Register Template**

The Asset Register Template (refer to Appendix E) is a powerful tool that provides a systematic methodology for documenting assets, evaluating their condition and value, and comprehending their significance to business operations. Crafted with an emphasis on simplicity and clarity, this template assists small enterprises in maintaining an accurate inventory, facilitating efficient resource allocation, and informed decision-making related to maintenance, upgrades, or disposals. The design encourages transparency and accountability, empowering organizations to manage their assets proficiently while adhering to financial and regulatory obligations. The following section outlines the essential data to be recorded in the asset register.

Asset Register		
Asset ID	Owner	Business Impact
Asset Type	Purchase Date	Disposal Date
Description	Condition	Notes/Updates
Location	Value (USD)	

Figure 4b: MCSF Asset Register Template Structure, Source: (Original Work)

**Asset ID:** Each asset is assigned a unique identifier (e.g., A0001), which facilitates efficient tracking and referencing within the inventory system. This system helps prevent confusion that may arise from similar assets.

**Asset Type:** This categorization classifies the asset into relevant categories such as laptop, mobile device, website, or application. Such classification not only enhances asset organization but also streamlines maintenance schedules, making the process more organized and efficient. It also supports the bulk management of assets within similar categories.

**Description:** The asset is described clearly and concisely, and it may encompass specific models, configurations, or features. For instance, "Dell XPS 13 with 16GB RAM and 512GB SSD."

**Location:** This field captures the physical or virtual location of the asset, such as "Main Office," "Employee Home," or "Cloud Server." Accurate location information is essential for effective asset tracking, audits, and logistics planning, particularly for assets distributed across multiple locations.



**Owner:** This role is of the utmost importance, as it refers to the individual, team, or department accountable for the asset's management. Designating ownership fosters accountability and establishes a specific point of contact for any issues, maintenance, or updates pertinent to the asset. The role of an owner is crucial to the success of the asset management process.

**Purchase Date:** This is a key piece of information in asset management, as it records the date when the asset was acquired (e.g. 1st March 2024). It plays a crucial role in warranty monitoring, depreciation assessments, budgeting for replacements, and understanding the asset's life cycle.

**Condition:** This is not just a mere status update indeed, but a crucial responsibility. It denotes the current status of the asset, categorized as "Needs Replacement," "Fair," "Good," "Excellent," or "N/A" for assets where condition assessment may not be applicable (such as software licenses). Evaluating the condition is essential for effective planning regarding maintenance, upgrades, or disposals.

**Value (USD):** Indicates the monetary value of the asset, either at the time of purchase or its current estimated worth. This information is crucial for financial accounting, insurance considerations, and assessing the financial repercussions of asset loss or impairment.

**Business Impact:** Evaluates the significance of the asset to business operations, categorized as "critical," "high," "medium," or "low." This classification helps prioritize assets for maintenance, security, and contingency planning, ensuring that essential assets receive the necessary attention.

**Disposal Date:** Records the anticipated or actual asset disposal date (e.g., 01 March 2027). Monitoring disposal dates facilitates lifecycle management, ensures environmental compliance, and aids in budgeting for asset replacements.

**Notes/Updates:** Provides space for documenting any modifications or updates related to the asset, such as "Updated OS on 01-September-2024" or "Transferred to Marketing Department on 15-August-2024." This feature ensures that the asset register reflects the most current information, supporting effective asset management.

#### 4.4.3 Common Controls List

The Common Controls List (refer to Appendix F) aims to provide small businesses with standardized security controls that address essential cybersecurity risks. These controls encompass various aspects of cybersecurity, including access management to data protection, and are adaptable based on the size and risk profile of the business. The framework prioritizes simplicity and practicality, enabling small businesses with limited resources to implement adequate security measures. Below is an outline of how the standard controls are structured:

Common Controls List		
Control #	Control Category	Baseline - Low
Notes	Control Description	Baseline - Medium

Figure 4c: MCSF Common Controls List Structure, Source: (Original Work)

**Control Categories and Descriptions:** Each control in the list is categorized based on its role in safeguarding critical business systems and data. The categories comprise access control, authentication, data encryption, incident response, security awareness training, and business continuity. Each control description is crafted to provide a clear understanding and guidance on its purpose within the cybersecurity framework.

**Baseline Levels: Low and Medium:** The controls are designed with a focus on flexibility, offering a two-tiered baseline - Low and Medium - thereby enabling organizations to select the level of security that aligns with their operational requirements:

- **Low Baseline:** This tier comprises minimalistic controls intended for organizations with constrained resources or lower risk profiles. It provides essential protections such as basic user permissions and quarterly patch updates.
- **Medium Baseline:** This elevated tier delivers enhanced security measures that remain accessible for small businesses while offering more comprehensive protection. Notable features at this level include multi-factor authentication (MFA) for all users and enterprise-grade antivirus solutions.
- Some examples of Key Controls are as follows:
  - **Access Control (CC-01):** The management of user access based on clearly defined roles and responsibilities is a fundamental element in the protection of critical systems. For small enterprises, the Low baseline involves basic user permissions, with administrative access granted solely to key personnel. In contrast, the Medium baseline necessitates the implementation of Role-Based Access Control (RBAC), accompanied by periodic reviews of access rights to ensure the effective management of sensitive information.
  - **Security Awareness Training (CC-08):** Human error represents a substantial risk factor within the sphere of cybersecurity. The Low baseline encompasses fundamental annual security training for all staff members, whereas the Medium baseline includes more comprehensive structured training programs featuring phishing simulations, thereby keeping employees informed about current threats.

- **Third-Party Risk Management (CC-11):** It is imperative to evaluate the security risks associated with vendors and partners that manage sensitive data. The Low baseline focuses on conducting basic assessments of vendors, while the Medium baseline incorporates formal vendor agreements and periodic audits, ensuring that relationships with third parties do not introduce vulnerabilities.

**Notes Section for Additional Guidance:** Each control features a dedicated notes section offering insights and recommendations for organizations to consider. For instance, it emphasizes the necessity of reviewing access permissions following role changes (CC-01) and the importance of conducting periodic testing of data restoration capabilities (CC-04). This ensures that organizations not only implement these controls effectively but also maintain ongoing oversight and assessment.

#### 4.4.4 Information Types for System Categorization List

The Information Types List (refer to Appendix G) serves as a systematic framework for small businesses to classify their data based on sensitivity, legal implications, operational significance, and the potential business impact of compromise. This categorization enables organizations to focus their data protection efforts on assets with the highest risk, including personally identifiable information (PII), financial records, and intellectual property. The structure is as follows:

Information Type List		
INF #	Description	Example of Impact
Information Type	Risk Category	Confidentiality Level

Figure 4d: MCSF Information Types List Structure, Source: (Original Work)

**Information Type (INF):** A concise label that distinctly identifies the specific data category.

**Description:** An overview detailing the characteristics of the data type and its relevance within the operational context of the business.

**Risk Category:** Primary risk classifications associated with the information encompassing privacy, financial, operational, legal, and cybersecurity.

**Example of Impact:** Real-world scenarios that depict the potential consequences for the business in the event of a data breach, loss, or mishandling.

**Confidentiality Level:** A rating system (e.g., High, Medium, Low) indicating the sensitivity of the data and the requisite level of protective measures needed.

**Examples of Key Information Types:**

- Financial Data
  - Risk Category: Financial, Compliance
  - Impact: Unauthorized access poses a significant risk of fraud, potential fiscal losses, and adverse reputational consequences.
  - Confidentiality Level: High
- Customer Information
  - Risk Category: Privacy, Operational
  - Impact: Compromise of customer data could significantly undermine customer trust and inflict reputational damage on the organization.
  - Confidentiality Level: Medium-High

**System Categorization:** By systematically categorizing information based on associated risks and impacts, small businesses can adopt a tiered approach to data security. This framework ensures that highly sensitive information, such as Personally Identifiable Information (PII), financial data, and intellectual property, receives the highest level of security controls. Conversely, less critical data types, including marketing metrics or website information, can be adequately secured using less resource-intensive measures while maintaining a focus on risk management.

#### 4.4.5 Risk Register Template

The Risk Register Template (refer to Appendix H) serves as an essential instrument for small businesses aiming to track and manage risks systematically. It provides a clear and organized framework for documenting risks, evaluating their potential impacts, and monitoring mitigation strategies. This template is structured to assist small businesses in prioritizing risks and ensuring that effective control measures are established, even when resources are limited. Its design enhances transparency and accountability, thereby facilitating proactive risk management.

Risk Register			
Risk ID	Likelihood (1-5)		
Risk Category	Impact (1-5)	Monitoring Freq	Control Measures
Risk Description	Risk Level	Notes/Updates	Mitigation Status
Date Identified	Assessment Date	Review Date	Due Date
Risk Owner	Assessor	Reviewer	Control Owner

Figure 4e: MCSF Risk Register Structure, Source: (Original Work)

**Risk Specifications:** This template section captures the fundamental details associated with each identified risk. It is intended to enable small businesses to maintain a comprehensive and current record of risks while ensuring consistent evaluation and monitoring.

- **Risk ID:** A distinctive identifier assigned to each risk (e.g., R0001), which aids in the efficient tracking and referencing of risks.
- **Risk Category:** Classifies the risk into pertinent categories, such as Operational, Financial, Cybersecurity, or Compliance, to facilitate prioritization and effective allocation of resources.
- **Risk Description:** A succinct yet comprehensive summary of the identified risk, encompassing potential cybersecurity threats, operational bottlenecks, or financial instability.
- **Date Identified:** The timestamp noting when the risk was initially detected, providing a historical benchmark for tracking purposes.
- **Risk Owner:** The designated individual, team, or department tasked with the oversight and management of the specific risk, thereby fostering accountability and establishing a clear point of contact.
- **Likelihood (1-5):** A quantitative assessment representing the probability of the risk occurring, rated on a scale where 1 denotes minimal likelihood and 5 indicates a high likelihood.
- **Impact (1-5):** A qualitative measurement of the potential consequences on the organization, with 1 indicating negligible impact and 5 signifying a critical, high-impact risk.

- **Risk Level:** An aggregated metric derived from the likelihood and impact scores, categorizing the risk into tiers such as High, Medium, or Low. This facilitates the prioritization of risks based on severity.
- **Assessment Date:** Logs the most recent risk assessment date, ensuring current evaluations and fostering proactive risk management practices.
- **Assessor:** The individual or team responsible for conducting the risk assessment, offering a transparent record of those engaged in the evaluation process.
- **Monitoring Frequency:** Defines the interval at which the risk is reviewed and monitored (e.g., Monthly, Quarterly), ensuring constant oversight and the effectiveness of mitigation strategies.
- **Review Date:** Captures the most recent date on which the risk was evaluated, underpinning ongoing vigilance and management.
- **Reviewer:** Identifies the individual or team conducting the latest review, enhancing transparency and accountability in the risk management process.
- **Notes/Updates:** A section designated for documenting any risk profile modifications, mitigation tactics revisions, or new insights. This ensures the risk register remains adaptive and responsive to changing risk landscapes.

**Controls Addressing The Risks:** This section outlines the controls and mitigation strategies established to address identified risks, focusing on monitoring their status to ensure timely execution, which is crucial for small enterprises operating with constrained resources.

- **Control Measures:** This component enumerates the preventive or corrective actions undertaken to mitigate risks. Such measures may encompass technical solutions (e.g., deploying firewalls), operational modifications (e.g., supplier



diversification), or procedural enhancements (e.g., instituting regular security audits).

- **Mitigation Status:** This tracks the advancement of the mitigation actions, categorizing their state as In Progress, Completed, or Not Started. This allows organizations to oversee control measures and prioritize actions according to the risk's severity.
- **Control Owner:** This identifies the individual or team accountable for executing the control measures. Emphasizing the role of the controlling owner fosters a sense of responsibility and accountability in the risk mitigation process.
- **Due Date:** This specifies a target completion date for implementing control measures, facilitating effective scheduling, and proactive risk management.

#### **4.5 Thematic Analysis of Interviews on the MCSF**

The thematic analysis of interview responses revealed several key themes indicating that a minimalistic cybersecurity framework effectively accommodates the needs of small businesses and startups. Notably, participants said that, unlike extensive frameworks such as the NIST Cybersecurity Framework (CSF) and ISO/IEC 27001, which they perceived as overly complex and resource-demanding, the minimalist framework offered a pragmatic and attainable solution. Despite engaging with experts over a three-month consultation period, small business owners found that even the simplified iterations of established frameworks did not adequately address their specific challenges. The novel minimalistic framework received a commendation for its user-centric design, clarity, and alignment with operational priorities, enabling independent implementation and management of cybersecurity practices, thereby empowering small business owners and

startups to take control of their cybersecurity. The following analysis is the principal themes derived from the interviews:

#### **4.5.1 Enhanced Accessibility and Comprehension**

**Clarity of Language and Terminology:** Participants collectively announced that the minimalistic framework significantly enhanced accessibility compared to traditional frameworks like NIST CSF and ISO 27001. They emphasized the impact of plain language and the deliberate omission of technical jargon as critical factors that fostered understanding. One participant noted, "The language was straightforward; I did not need a cybersecurity background to grasp the concepts. Your one-day training was more than enough."

**User-Friendly Guidance and Instructions:** The step-by-step guidance articulated within the framework received appreciation for its clarity and practicality. One participant remarked, "The instructions were clear and actionable. I experienced confusion with NIST previously, but within the MCF, I now understand precisely what actions to undertake without second-guessing."

#### **4.5.2 Practical Implementation with Limited Resources**

**Manageable Resource Requirements:** Participants identified the framework's implementation as feasible within their current resource limitations. The modular design enabled them to prioritize essential components without experiencing overwhelming complexity. One participant stated, "We could easily implement the core components without employing additional staff or consultants. We already know what it has, but now it is documented and appears more reliable."

**Minimal Disruption to Business Operations:** The framework is combined effectively with existing business processes, thereby minimizing operational disruptions. One participant commented, "It did not interfere with our daily operations. In fact, it enhanced our workflows."

#### **4.5.3 Effective Risk Management**

**Simplified Risk Identification and Prioritization:** Risk identification has proven a powerful tool, empowering organizations to recognize and prioritize cybersecurity risks pertinent to their specific operational contexts. One participant remarked, "The simplified risk assessment made it easier to identify our vulnerabilities, giving us a greater sense of control."

**Utilization of Templates and Tools:** Implementing resources such as the Risk Management Strategy and the Risk Register has not only played a crucial role in structuring risk management initiatives. It has also transformed the way we approach risk. As a participant stated, "The templates were truly transformative. They provided a strong foundation for our risk management strategy, giving us a new sense of optimism."

#### **4.5.4 Improved Cybersecurity Posture**

**Implementation of Basic Protective Measures:** The participants successfully executed fundamental protective measures, resulting in immediate enhancements to their cybersecurity posture. As one participant noted, "By enforcing multi-factor authentication and utilizing antivirus solutions, we observed a considerable reduction in security issues, which is a positive development." This immediate improvement provides a sense of reassurance and security.

**Preparedness for Cybersecurity Incidents:** Establishing an incident response protocol significantly bolstered participants' confidence in their ability to address potential threats, providing a sense of security. One participant expressed, "We now possess a clear plan to follow in the event of an incident; everything is documented, and I feel more secure and confident."

#### **4.5.5 Empowerment and Independence**

**Self-Sufficiency in Cybersecurity Management:** Participants reported a newfound capability in managing cybersecurity protocols autonomously, significantly decreasing their dependence on external consultants. One participant noted, "We no longer feel helpless. We can handle cybersecurity ourselves now."

**Augmented Knowledge and Skillset:** The implementation of the framework notably elevated the cybersecurity acumen of their teams. One participant stated, "Our team is more aware of cybersecurity risks and possesses the skills to mitigate them effectively."

#### **4.5.6 Alignment with Business Priorities**

**Emphasis on Growth and Operational Efficiency:** The framework's streamlined nature effectively aligned with the organization's primary objectives: growth and operational efficiency. A participant commented, "It did not distract us from our core business objectives. Instead, it supported them by providing insights relevant to our business needs."

**Scalability and Flexibility of Design:** The framework's modular architecture allowed for scalable implementation, enabling organizations to integrate additional components as they expand. One participant said, "We can add more controls when ready,

which is ideal for our growth plans. For now, we wanted to start with the bare minimum, and this framework provides that foundation."

In this chapter, we have meticulously analyzed the varied dimensions of cybersecurity understanding and implementation among small businesses. We began by assessing their initial awareness and preparedness, outlining the evident discrepancies between knowledge and practical application. The study embarked on a journey through different frameworks, identifying persistent barriers and highlighting the substantial challenges businesses face despite heightened awareness. As we transitioned to the development and application of a minimalistic cybersecurity framework, the analysis uncovered a marked improvement in accessibility and comprehension. The results suggest an encouraging trend towards empowerment and self-sufficiency among small business stakeholders.

## CHAPTER V: CONCLUSIONS & RECOMENDATIONS

Let us dive into what we learned about keeping small businesses safe in the digital world. Our research mixed different methods to paint a clear picture, and what we found was eye-opening - while business owners know cybersecurity matters, many struggle to put effective safeguards in place. We will walk through how we built and tested our streamlined security approach, the Minimalist Cyber Security Framework. Think of it as a practical toolkit that works with limited resources and doesn't require deep IT knowledge. After running training sessions and working directly with businesses, patterns emerged. Money's tight, technical know-how is often scarce, but that doesn't mean cybersecurity is impossible. We discovered ways to work around these challenges. Throughout this chapter, we'll map out practical steps for better security that fit how small businesses operate and grow. No fancy jargon or impossible requirements- just real solutions that work in the real world. By looking at what works and what doesn't, we're lighting the way forward for smaller companies to protect themselves without breaking the bank or getting lost in technical complexity.

### **5.1 Summary of Findings**

This research examined the complex cybersecurity landscape faced by small businesses, focusing on the challenges they encounter and the potential for tailored frameworks to address these issues. Through a detailed mixed-method approach involving surveys, training sessions, consultations, and interviews, several critical findings were uncovered:

Initial surveys revealed that while small business owners demonstrate moderate awareness of cybersecurity risks, there is a notable gap in the implementation of robust measures. Specifically, 67% of respondents acknowledged cybersecurity as a moderate to

high priority, yet most had not moved beyond basic practices such as antivirus software usage. This highlights a critical challenge: advancing from rudimentary awareness to more proactive and sophisticated cybersecurity strategies.

The training and consultation phases significantly improved participants' theoretical understanding and practical application of cybersecurity frameworks. Despite a month-long training on the NIST Cybersecurity Framework (CSF) and ISO/IEC 27001, many businesses struggled to translate theoretical knowledge into actionable strategies. Post-training surveys reflected modest progress, with increased awareness failing to fully address implementation challenges. However, follow-up consultations offered tailored guidance, which helped bridge gaps in technical expertise and enhanced businesses' capacity to manage cybersecurity independently.

One of the study's key outcomes was the creation of the Minimalistic Cyber Security Framework, tailored specifically for small businesses. This framework simplifies cybersecurity into essential components, making it accessible for organizations with limited resources and technical know-how. It prioritizes fundamental aspects like risk identification, basic protective measures, and incident response protocols, presented in user-friendly language and formats to enable independent implementation by small business owners.

Thematic analysis of post-consultation interviews provided deeper insights into the obstacles small businesses face. Common barriers include the overwhelming complexity of existing frameworks, resource limitations, difficulties aligning cybersecurity with business priorities, and persistent perceptions of cybersecurity as a lower priority during initial growth stages. The Minimalistic Cyber Security Framework effectively addressed these challenges by offering a resource-efficient, adaptable solution that aligns with the operational and growth needs of small businesses.

## **5.2 Addressing the Research Objective**

This research effectively explored cyber security assurance practices in small businesses, highlighting distinctive key hardships and challenges with the current frameworks. Here's an expanded analysis of how each objective was addressed through this study:

### **Objective 1: Evaluate the existing level of awareness regarding cybersecurity risks and vulnerabilities**

This objective focused on understanding the awareness of small business owners regarding cybersecurity risks and how well they cope with the threats. The survey results offered some eye-opening insights. While 67% of the businesses surveyed had moderate awareness of cybersecurity threats, only a minimum number had implemented security measures. Most of their awareness was limited to basic threats like phishing and malware, with many underestimating the dangers of more complex attacks, such as ransomware or insider threats. Through training sessions and consultations, this gap became even more evident, underscoring the need for targeted initiatives that address the specific challenges small businesses encounter in the real world.

### **Objective 2: Examine the common cybersecurity practices currently adopted by small businesses**

Exploring the cybersecurity practices of small businesses provided critical insight into their operations. The findings highlighted major reliance on basic protections like antivirus software and firewalls, with only 20% of businesses adopting more advanced measures such as multi-factor authentication or employee training. Post-survey training sessions showed slight improvements in these practices, but barriers such as limited resources and technical expertise remained significant. These results stress the importance



of equipping businesses with practical skills and simplified tools to strengthen their cybersecurity defenses.

**Objective 3: Investigate which frameworks are most relevant and feasible for adoption by small businesses**

A key focus of this research was to identify cybersecurity frameworks most suited for small businesses. The study examined frameworks like the NIST Cybersecurity Framework (CSF), ISO/IEC 27001, and the NIST Risk Management Framework (RMF), uncovering significant challenges in their implementation due to their complexity and resource-intensive nature. The development of the Minimalistic Cyber Security Framework emerged from these findings, offering an accessible solution tailored to small business environments. This simplified framework underscores the need for adaptability and practicality in cybersecurity approaches for resource-constrained organizations.

**Objective 4: Identify the primary barriers faced by small businesses in implementing these frameworks**

The study identified several barriers to implementing cybersecurity measures, limited budgets (35%), lack of technical expertise (40%), and a perception of low risk (25%). Interviews conducted during the consultation phase revealed further challenges, such as difficulty in understanding technical jargon and integrating frameworks with existing operations. These findings highlighted a critical gap, underlining the need for frameworks that are both simple and modular, allowing businesses to incrementally adopt more complex measures as their resources and needs grow.

**Objective 5: Develop and implement training programs aimed at increasing cybersecurity awareness and framework adoption among small business owners**

Focused training programs were developed and implemented to improve cybersecurity awareness and support framework adoption. These programs focused on

practical, real-world applications and included case studies relevant to small businesses. Feedback from participants indicated that hands-on workshops and relatable examples were particularly effective in increasing awareness and engagement. While many participants reported a greater readiness to implement cybersecurity measures, ongoing support was identified as critical to translating theoretical knowledge into sustained practice.

**Objective 6: Provide expert consultations to tailor cybersecurity measures to the unique needs of small businesses**

Expert consultations played a crucial role in translating the Minimalistic Cyber Security Framework into actionable measures. These sessions were tailored to the unique needs and constraints of individual businesses, providing hands-on support that went beyond training. This personalized approach facilitated the customization of security measures, enabling businesses to view cybersecurity as an attainable goal rather than an overwhelming task. Feedback from participants highlighted improvements in their ability to independently implement practical cybersecurity measures, showcasing the effectiveness of targeted, continuous support.

**Objective 7: Utilize grounded theory to create a streamlined cybersecurity framework based on practical insights**

Grounded theory was used to design a cybersecurity framework made for small businesses, focusing on simplicity and practicality. This method involved chronologically gathering and analyzing data from consultations, training sessions, and real-world implementation experiences. By zeroing in on the common challenges and effective strategies uncovered during these interactions, the framework was designed to address the key issues small businesses face. The outcome is a practical and accessible tool that helps

small businesses enhance their cybersecurity with confidence, without adding unnecessary complexities.

**Objective 8: Validate the practicality, usability, and impact of the newly developed framework in real-world small business settings.**

Validation of the Minimalistic Cyber Security Framework was achieved through feedback from interviews and practical application data. Small businesses reported marked improvements in their security posture, incident preparedness, and understanding of cybersecurity risks. The framework's simplicity and modular structure were particularly praised, as they allowed for easy adoption and gradual scaling. Participants noted that the user-friendly design enabled them to manage cybersecurity independently, reflecting a significant shift toward self-sufficiency and resilience.

By methodically addressing all research objectives, this study not only highlighted critical gaps in current cybersecurity practices but also offered practical solutions to address them. Through focused interventions and an emphasis on accessibility and practicality, the research has made a meaningful contribution to improving the cybersecurity landscape for small businesses, providing a sustainable path toward enhanced protection against cyber threats.

### **5.3 Recommendations**

The findings of this study highlight critical gaps in the cybersecurity practices of small businesses and offer practical solutions to improve their defenses. These suggestions focus on making cybersecurity accessible, scalable, and simple to meet the specific needs

of small businesses/enterprises. They are directed at policymakers, business owners, industry leaders, and the broader cybersecurity community.

### **5.3.1 Policy Recommendations**

Governments should provide financial support, such as tax relief, and grants/subsidies, to make cybersecurity investments more affordable for small businesses. This would ease the financial burden and motivate businesses to adopt stronger security measures.

Introduce regulations requiring regular cybersecurity audits. These audits would give businesses clear benchmarks to evaluate their security and drive ongoing improvements.

Policymakers should create straightforward, easy-to-follow cybersecurity compliance guidelines designed for small businesses. This would reduce confusion and encourage better compliance without sacrificing security.

Develop industry-specific rules that address the unique risks and needs of different sectors, allowing businesses to focus on relevant threats.

### **5.3.2 Framework Adoption Strategies**

Support the adoption of modular frameworks like the Minimalistic Cyber Security Framework introduced in this research. These frameworks let businesses start with basic protections and gradually add more as they grow.

Advocate for frameworks that fit naturally into daily operations, ensuring they enhance productivity rather than creating additional challenges.

Encourage partnerships between businesses, cybersecurity vendors, and industry groups to ensure affordable access to security tools and services. Collaboration can also help solve shared challenges more efficiently.

Create alliances or consortia where businesses can share threat intelligence and best practices, building collective defenses against cyberattacks.

### **5.3.3 Training and Education Initiatives**

Small businesses should provide regular cybersecurity training to employees, keeping them updated on the latest threats and prevention strategies.

Focus training on practical topics like identifying phishing attempts, securing data, and responding to security incidents.

Offer training through digital platforms to make it accessible and flexible. Interactive sessions, simulations, and scenario-based learning can help employees retain what they learn.

Encourage participation in workshops, webinars, and hands-on boot camps to build practical cybersecurity skills.

### **5.3.4 Enhancing Public Awareness and Community Engagement**

Launch national campaigns to educate small businesses about cybersecurity threats and the importance of proactive defenses. Use platforms like social media and local media outlets to spread the message.

Set up local cybersecurity forums where business owners can share experiences, challenges, and solutions.

Small businesses should connect with local cybersecurity professionals and groups to seek advice and support.

Partner with universities or technology hubs to create programs where experts and students provide consultation and practical solutions to small businesses.

### **5.3.5 Future Research and Development**

Research to understand the unique cybersecurity challenges of industries like healthcare, retail, and manufacturing. Develop targeted strategies to address these issues.

Publish case studies showcasing how different sectors have successfully implemented cybersecurity measures to guide others.

Study the impact of new technologies like AI, IoT, and machine learning on cybersecurity. Use these insights to design defenses against emerging risks.

Explore affordable ways for small businesses to adopt advanced security tools without overextending their budgets.

Encourage businesses to view cybersecurity as a core part of their strategy, aligning security efforts with overall business goals.

Develop tools and frameworks that make it easier for businesses to incorporate cybersecurity into their planning and operations.

### **5.4 Limitations of the Study**

While this research offers valuable insights into improving cybersecurity practices for small businesses, it is also important to recognize the limitations that may influence the interpretation and application of its findings. Identifying these limitations not only contextualizes the study but also highlights areas for future research. These limitations can

be broadly grouped into geographical scope, evolving threats, participant resource constraints, sample diversity, and methodological choices.

#### **5.4.1 Geographical Scope**

A key limitation of this study is its primary focus on small businesses located in the United States. This restricted scope means the findings might not fully reflect the realities of businesses in other regions, where regulatory frameworks, cultural factors, and technology adoption differ. For instance, small businesses in countries with varying economic conditions or distinct cybersecurity legislation may encounter unique challenges not addressed in this research. Although the study incorporated input from international experts to enhance the relevance of its recommendations, the framework's applicability may still vary across regions. Future studies should consider conducting comparative research across multiple countries to identify both universal solutions and region-specific cybersecurity strategies.

#### **5.4.2 Evolving Cybersecurity Threats**

The dynamic nature of cybersecurity, with its ever-changing technologies and threats, poses other limitations too. This research captures the state of cybersecurity challenges as they existed during the study period. However, as small businesses increasingly adopt emerging technologies like IoT, AI, and blockchain, new vulnerabilities and risks will surface. Consequently, the strategies and recommendations outlined in this study may require regular updates to remain effective. Long-term research that monitors these technological advancements and evolving threats would ensure that cybersecurity frameworks stay relevant and adaptable.

### **5.4.3 Resource Constraints of Participants**

The small businesses involved in this study exhibited significant variation in their resources, technological capabilities, and cybersecurity readiness. This variation influenced their ability to implement the proposed Minimalistic Cyber Security Framework. Businesses with limited resources often struggled to adopt even basic measures, while those with advanced infrastructures needed more customized solutions. Although the study included tailored consultations and training to address these disparities, future research should delve deeper into segmenting small businesses based on their resources and capabilities. Such segmentation could help develop more targeted recommendations that address the specific needs of each group.

### **5.4.4 Diversity and Size of the Sample**

This research's sample consisted of 25 small businesses, which, while allowing for an in-depth analysis, limits the adaptability of its findings. The vast diversity within the small business sector, including differences in industries, operating models, and cybersecurity maturity, means that the insights gained from this sample may not fully capture all the challenges. Expanding the sample size and including a wider variety of businesses from different sectors could provide a more comprehensive understanding of the cybersecurity needs and solutions applicable to each industry.

### **5.4.5 Methodological Choices**

The mixed-methods approach used in this research, while effective in offering a holistic perspective, comes with its own set of limitations. The chronological nature of data collection meant that some key insights emerged later in the process, potentially limiting



their influence on earlier phases of the study. Additionally, self-reported data from surveys and interviews introduces the possibility of bias, such as participants providing answers, they believe are expected rather than their actual practices. To address this, future research could incorporate observational methods or case studies for a more objective assessment of cybersecurity practices. Advanced techniques like machine learning could also be used to analyze security practices and outcomes, offering deeper quantitative insights.

#### **5.4.6 Focus on Specific Frameworks**

This study concentrated on evaluating widely recognized frameworks like the NIST Cybersecurity Framework (CSF) and ISO/IEC 27001 due to their comprehensive nature. While these frameworks were suitable for the study's objectives, this focus limited the exploration of other potentially valuable or emerging frameworks. Expanding future research to include lesser-known or hybrid models could provide insights into alternative approaches that might better address the specific needs of small businesses.

By acknowledging these limitations, this study aims to provide a transparent and realistic perspective on its findings. Addressing these gaps through further research will help refine the understanding of small businesses' cybersecurity needs, fostering the development of more effective and adaptable solutions across diverse contexts.

### **5.5 Final Thoughts**

Small businesses keep our economy moving, but they need the right tools to stay safe in today's digital world. This research highlights the pressing need to strengthen cybersecurity in this sector and takes a meaningful step toward equipping small enterprises with the tools they need to safeguard their digital futures.

#### **5.5.1 The Imperative for Tailored Cybersecurity Solutions**

One of the key insights from this study is the clear need for cybersecurity frameworks that cater specifically to the realities of small businesses. Many of the existing frameworks, though comprehensive, are often too complex or resource-intensive for smaller businesses. The Minimalistic Cyber Security Framework developed through this research offers a more practical alternative, focusing on simplicity, flexibility, and affordability. It shows that cybersecurity does not have to be overwhelming—it can be an easy-to-adopt part of everyday business operations, tailored to fit the unique needs of small businesses.

### **5.5.2 A Call for Continued Engagement and Collaboration**

The findings emphasize the importance of collaboration among all the key players: governments, industry leaders, academic institutions, and cybersecurity experts. Real change will come from collective actions. Governments can play their part by offering financial support and crafting policies that encourage small businesses to prioritize cybersecurity. Industry groups and educational institutions can provide platforms for knowledge-sharing, training, and cooperative problem-solving.

Cybersecurity is not a one-time fix. It is an ongoing process that requires regular attention and adaptation. Collaborating with universities can help keep small businesses informed and equipped, while forums, webinars, and online communities can create opportunities for shared learning and networking. These efforts can foster a mindset where cybersecurity becomes an integral and continuous part of business operations.

### **5.5.3 Bridging the Knowledge and Resource Gap**

Though small business owners are aware of cybersecurity risks, turning that awareness into action remains a challenge. The solution lies in education. Training

programs need to focus on delivering practical, hands-on learning that aligns with the realities of running a small business. Cybersecurity should not feel like an extra burden but rather a natural extension of daily operations.

Limited resources are another significant hurdle. Many small businesses operate on squeezed budgets, so scalable and cost-effective solutions—like cloud-based security tools are crucial. By encouraging a gradual, chronological approach to improve cybersecurity, small businesses can enhance their defenses without stretching their resources too thin.

#### **5.5.4 The Road Ahead: Embracing Innovation and Agility**

Small businesses must remain agile and ready to embrace new technologies and strategies to counteract emerging cyber threats. The rapid pace of technological change requires businesses to adopt tools like artificial intelligence, machine learning, and blockchain to stay ahead. These technologies need to be accessible and affordable to truly benefit small businesses.

At the same time, cybersecurity frameworks must evolve to keep up with changing threats. Feedback from small businesses will be invaluable in refining these frameworks and ensuring they remain practical and effective. The key will be staying adaptable and open to new ideas while maintaining a focus on what works best for small enterprises.

#### **5.5.5 Emphasizing a Shared Responsibility**

Finally, strengthening cybersecurity in small businesses is a shared responsibility. It is not just about individual efforts; it requires a collective commitment from governments, industries, and communities. By working together, we can create an environment where small businesses are better equipped to handle the challenges of the digital era.

Though this research offers a significant contribution, it is only one part of a broader effort to build a more secure future for small businesses. By fostering collaboration, embracing innovation, and focusing on practical solutions, we can ensure that small businesses are not just surviving but thriving in an increasingly interconnected arena. The simple Cyber Security Framework serves as a reminder that even the most modest, well-thought-out solutions can make a big difference. As it continues to evolve, it will remain a valuable ally for small businesses in their journey toward stronger cybersecurity.

APPENDIX A:  
SURVEY QUESTIONS FOR UNDERSTANDING CYBERSECURITY AWARENESS  
AND READINESS AMONG SMALL BUSINESS OWNERS

**Introduction:**

We are conducting a survey as part of a doctoral research project to understand the level of awareness and preparedness small business owners have regarding cybersecurity and their knowledge of cybersecurity frameworks. The survey will take about 10–15 minutes to complete. Your responses are completely anonymous and will help in shaping effective cybersecurity strategies for small businesses. Thank you for your time!

Section 1: Business Demographics

1. What is the primary industry of your business?
  - a. Retail
  - b. Healthcare
  - c. Manufacturing
  - d. Professional Services
  - e. Technology
  - f. Other (please specify): \_\_\_\_\_
  
2. How many employees does your business have?
  - a. 1–5
  - b. 6–20
  - c. 21–50
  - d. 51–100
  - e. 101+

3. What is your role in the company?
  - a. Owner
  - b. Manager
  - c. IT/Admin Lead
  - d. Other (please specify): \_\_\_\_\_
4. How long has your business been operational?
  - a. Less than 1 year
  - b. 1–3 years
  - c. 4–10 years
  - d. More than 10 years

## **Section 2: Cybersecurity Awareness**

5. How would you rate your overall awareness of cybersecurity risks for your business?
  - a. Very low
  - b. Low
  - c. Moderate
  - d. High
  - e. ry high
6. Have you experienced any cybersecurity incident(s) in the past?
  - a. Yes
  - b. No
7. If yes, what was the nature of the incident?
  - a. Data breach
  - b. Ransomware attack

- c. Phishing attack
  - d. Malware infection
  - e. Other (please specify): \_\_\_\_\_
8. How concerned are you about the potential impact of a cybersecurity incident on your business?
- a. Not concerned
  - b. Slightly concerned
  - c. Moderately concerned
  - d. Very concerned
  - e. Extremely concerned

### **Section 3: Cybersecurity Practices**

9. Does your business have any cybersecurity measures in place (e.g., firewalls, anti-virus software, regular backups)?
- a. Yes
  - b. No
  - c. Not sure
10. If yes, which of the following measures are implemented? (Select all that apply)
- a. Anti-virus software
  - b. Firewalls
  - c. Data encryption
  - d. Regular data backups
  - e. Multi-factor authentication (MFA)
  - f. Employee cybersecurity training
  - g. Cyber insurance

h. Other (please specify): \_\_\_\_\_

11. How frequently does your business review or update its cybersecurity measures?

- a. Never
- b. Every 6 months
- c. Annually
- d. Every 2–3 years
- e. Only after a cybersecurity incident

#### **Section 4: Knowledge of Cybersecurity Frameworks**

12. Are you aware of any cybersecurity frameworks or guidelines for small businesses?

- a. Yes
- b. No

13. If yes, which of the following frameworks are you familiar with? (Select all that apply)

- a. NIST Cybersecurity Framework
- b. ISO/IEC 27001
- c. CIS Controls
- d. PCI DSS
- e. Other (please specify): \_\_\_\_\_

14. Have you implemented any cybersecurity framework in your business?

- a. Yes
- b. No
- c. Currently in progress



15. If not, what are the primary barriers to implementing a cybersecurity framework?

(Select all that apply)

- a. Lack of awareness
- b. Lack of technical expertise
- c. Cost concerns
- d. Time constraints
- e. Perception of low-risk
- f. Other (please specify): \_\_\_\_\_

### **Section 5: Capability and Willingness**

16. How confident are you in your business's ability to implement a cybersecurity framework effectively?

- a. Not confident
- b. Slightly confident
- c. Moderately confident
- d. Very confident
- e. Extremely confident

17. Would you be willing to allocate resources (time, money, or personnel) to improve cybersecurity in your business?

- a. Yes
- b. No
- c. Maybe

18. If yes, which resources are you willing to invest? (Select all that apply)

- a. Hiring cybersecurity professionals
- b. Employee training

- c. Investing in cybersecurity tools/software
- d. Developing a cybersecurity policy
- e. Other (please specify): \_\_\_\_\_

19. How much do you currently invest (or would be willing to invest) annually in cybersecurity?

- a. Less than \$1,000
- b. \$1,000 – \$5,000
- c. \$5,000 – \$10,000
- d. More than \$10,000
- e. Not sure

### **Section 6: Additional Insights**

20. Do you believe that implementing a cybersecurity framework would positively impact your business operations?

- a. Yes
- b. No
- c. Maybe

21. What are your main cybersecurity concerns for the future? (Open-ended)

22. Would you like to receive more information or assistance regarding cybersecurity frameworks?

- a. Yes
- b. No

### **Conclusion:**

Thank you for participating in this survey. Your responses will contribute to valuable

research on cybersecurity practices among small businesses and help shape recommendations that can support businesses like yours in staying secure and resilient in today's digital landscape.

APPENDIX B:  
SURVEY QUESTIONS FOR ASSESSING SMALL BUSINESS UNDERSTANDING  
AND IMPLEMENTATION OF CYBERSECURITY FRAMEWORKS AFTER  
TRAINING FOR 1 MONTH

**Introduction:**

Thank you for participating in our second survey. Over the past month, we provided training on key cybersecurity frameworks—NIST Cybersecurity Framework (CSF), ISO/IEC 27001, and NIST Risk Management Framework (RMF). We are conducting this survey to evaluate your understanding of these frameworks, the progress you've made in implementing them, and any challenges you have encountered. Your feedback will help improve future initiatives aimed at enhancing cybersecurity in small businesses. The survey will take approximately 10 minutes to complete.

**Section 1: Understanding of Cybersecurity Frameworks**

1. How would you rate your understanding of the following frameworks after the training sessions? (Please select a rating for each framework.)
  - a. NIST Cybersecurity Framework (CSF)
    - i. No understanding
    - ii. Basic understanding
    - iii. Moderate understanding
    - iv. Good understanding
    - v. Comprehensive understanding

b. ISO/IEC 27001

- i. No understanding
- ii. Basic understanding
- iii. Moderate understanding
- iv. Good understanding
- v. Comprehensive understanding

c. NIST Risk Management Framework (RMF)

- i. No understanding
- ii. Basic understanding
- iii. Moderate understanding
- iv. Good understanding
- v. Comprehensive understanding

2. Do you feel confident in your ability to apply the NIST CSF in your business operations?

- a. Not confident
- b. Slightly confident
- c. Moderately confident
- d. Very confident
- e. Extremely confident

3. Do you feel confident in your ability to apply ISO/IEC 27001 in your business operations?

- a. Not confident

- b. Slightly confident
  - c. Moderately confident
  - d. Very confident
  - e. Extremely confident
4. Do you feel confident in your ability to apply the NIST RMF in your business operations?
- a. Not confident
  - b. Slightly confident
  - c. Moderately confident
  - d. Very confident
  - e. Extremely confident

## **Section 2: Implementation Progress**

5. Have you begun implementing any of the following frameworks in your business?  
(Please select all that apply.)
- a. NIST Cybersecurity Framework (CSF)
  - b. ISO/IEC 27001
  - c. NIST Risk Management Framework (RMF)
  - d. None
6. If you have started implementation, which steps have you completed for each framework? (Please select all that apply for each framework.)
- a. NIST Cybersecurity Framework (CSF)

- i. Identified key cybersecurity risks
- ii. Implemented basic security measures
- iii. Created an incident response plan
- iv. Ongoing monitoring of security controls
- v. Full implementation

b. ISO/IEC 27001

- i. Conducted risk assessments
- ii. Defined an information security policy
- iii. Identified necessary controls
- iv. Implemented a security management system (ISMS)
- v. Full implementation

c. NIST Risk Management Framework (RMF)

- i. Categorized information systems
- ii. Selected appropriate security controls
- iii. Implemented security controls
- iv. Conducted security assessment
- v. Full implementation

7. If you have not started implementation, what are the main reasons? (Select all that apply.)

- a. Lack of time
- b. Lack of technical expertise
- c. Cost concerns

- d. Unclear next steps
- e. Not a priority at this time
- f. Other (please specify): \_\_\_\_\_

### **Section 3: Challenges and Support Needs**

8. What challenges are you facing in implementing these frameworks? (Select all that apply.)
- a. Understanding the technical requirements
  - b. Limited budget for cybersecurity tools
  - c. Lack of internal expertise
  - d. Integration with existing systems
  - e. Lack of time or resources
  - f. No major challenges encountered
  - g. Other (please specify): \_\_\_\_\_
9. What kind of support would help you in implementing these frameworks? (Select all that apply.)
- a. Additional training or workshops
  - b. Access to cybersecurity experts/consultants
  - c. More affordable cybersecurity tools
  - d. Government or industry incentives
  - e. Clearer step-by-step guides
  - f. Other (please specify): \_\_\_\_\_



#### **Section 4: Business Impact and Future Plans**

10. Do you believe that implementing these frameworks will improve your business's cybersecurity posture?
- a. Strongly agree
  - b. Agree
  - c. Neutral
  - d. Disagree
  - e. Strongly disagree
11. Which cybersecurity framework do you find most relevant for your business?
- a. NIST Cybersecurity Framework (CSF)
  - b. ISO/IEC 27001
  - c. NIST Risk Management Framework (RMF)
  - d. All of them equally
  - e. None of them
12. Do you plan to fully implement any of these frameworks in the next 6 months?
- a. Yes
  - b. No
  - c. Maybe

#### **Section 5: Additional Insights**

13. What specific outcomes do you expect from implementing a cybersecurity framework? (Open-ended question)

14. What additional resources or support would you like to receive as you work toward implementing these frameworks? (Open-ended question)
15. Would you be interested in participating in follow-up sessions or receiving further training on advanced topics related to cybersecurity frameworks?
- a. Yes
  - b. No
  - c. Maybe

**Conclusion:**

Thank you for completing this survey. Your feedback is crucial in understanding the effectiveness of the training and the challenges small businesses face in adopting cybersecurity frameworks. Your responses will help inform future research and develop more targeted support for businesses like yours in enhancing cybersecurity.

APPENDIX C:  
INTERVIEW GUIDE FOR POST 3 MONTH CONSULTING ON CSF  
IMPLEMENTATION IN SMALL BUSINESSES

**Introduction:** Thank you for taking the time to speak with me today. As part of my PhD research, I've been working with small businesses like yours to implement the NIST Cybersecurity Framework (CSF). The goal of this interview is to understand your experience over the last three months, particularly how the consultation process helped with implementation, any challenges you faced, and the impact it has had on your business's cybersecurity posture. Your feedback is essential for improving future consultations and understanding how small businesses can better integrate cybersecurity frameworks. This interview should take about 45 minutes.

**A. Framework Understanding and Implementation Progress:**

1. How would you describe your overall understanding of the NIST CSF now compared to before the consulting process started?

Follow-up: Are there any particular areas of the framework that you feel especially confident in now?

2. Could you walk me through the steps your business has taken to implement the NIST CSF during the consultation period?

Follow-up: Which areas of the NIST CSF (e.g., Identify, Protect, Detect, Respond, Recover) have you been able to fully implement?

3. What specific changes have been made to your business operations as a result of implementing the NIST CSF?
4. Has your business developed any new policies or procedures based on the NIST CSF? If so, can you provide examples?

**B. Challenges Faced During Implementation:**

5. What challenges did you encounter during the process of implementing the NIST CSF with the consultant's help?

Follow-up: Were there any technical, financial, or operational challenges that made it difficult to adopt certain aspects of the framework?

6. How did you handle any resistance or difficulties from employees or stakeholders during the implementation process?
7. Was there any part of the NIST CSF that you found particularly difficult to understand or apply to your business? Why do you think that was the case?
8. Looking back, what would have helped you overcome these challenges more effectively?

**C. Impact and Benefits of NIST CSF:**

9. Since implementing the NIST CSF, have you noticed any improvements in your business's cybersecurity posture?

Follow-up: Can you provide examples of specific risks that have been mitigated or improvements in security practices?

10. Have you experienced any tangible benefits from implementing the NIST CSF (e.g., fewer incidents, better risk management, improved compliance)?

11. Do you feel that implementing the NIST CSF has provided a competitive advantage for your business in any way?

Follow-up: For example, has it helped build trust with customers or partners?

**D. Consultation Process Evaluation:**

12. How would you evaluate the consultation process overall?

Follow-up: What aspects of the consultation were the most helpful for your business?

13. Do you feel the consultant's guidance was effective in helping you understand and apply the NIST CSF? If so, what specific aspects were most beneficial?

14. Were there areas where you feel the consultation process could have been improved?

Follow-up: Were there any areas where you needed more support or clearer guidance?

15. Do you feel that three months was sufficient time to make meaningful progress on NIST CSF implementation? Why or why not?

**E. Closing Thoughts:**

16. Based on your experience, do you think your business is now better equipped to manage cybersecurity risks in the long term?

17. Looking ahead, do you plan to continue improving your cybersecurity efforts using the NIST CSF, or are there other frameworks you are considering adopting?
18. What advice would you give to other small business owners who are considering implementing the NIST CSF?
19. Is there anything else you would like to share about your experience with the NIST CSF implementation and consultation process?

**Closing Statement:** “Thank you so much for sharing your experiences and insights. Your feedback is incredibly valuable for my research and will help shape future consultations to better support small businesses like yours in enhancing their cybersecurity practices. If you have any additional thoughts after this interview, please feel free to reach out. Thanks again for your time and participation.”

APPENDIX D:  
RISK MANAGEMENT STRATEGY TEMPLATE

**1. Introduction**

At My Small Business Inc., we recognize that risk is an inherent part of doing business. Our Risk Management Strategy is designed to identify, assess, and manage risks to our operations, reputation, and information security. We are committed to protecting the privacy and security of our clients, employees, and partners while fostering a secure and compliant operating environment.

**2. Objectives**

The objectives of our Risk Management Strategy are to:

- A. Ensure business continuity and minimize disruptions.
- B. Protect our assets, including intellectual property, client data, and financial resources.
- C. Establish a proactive approach to identifying and mitigating risks.
- D. Comply with applicable laws, regulations, and industry standards.
- E. Provide a structured framework for managing information security and privacy risks.

**3. Risk Management Process**

Our risk management process follows these key steps:

- A. Regularly identify potential risks, including operational, financial, strategic, reputational, legal, and cybersecurity risks.
- B. Evaluate the likelihood and impact of identified risks using a risk matrix. Prioritize risks based on their severity.
- C. Develop and implement risk mitigation strategies that aim to reduce the likelihood and/or impact of risks. This may include policy updates, implementing security controls, employee training, and technological solutions.
- D. Continuously monitor and review risk factors and the effectiveness of mitigation measures. Regular audits and assessments will be conducted.
- E. Ensure that key stakeholders, including management, employees, and partners, are informed of the risks and the steps being taken to mitigate them.

#### **4. Information Security Risk Tolerance Statement**

My Small Business Inc. is committed to safeguarding sensitive information and ensuring the security of all digital and physical assets. We maintain a low tolerance for information security risks. Our business model involves handling sensitive client data, and any compromise in information security could harm our clients, damage our reputation, and disrupt our operations.

To manage information security risks effectively, we:

- A. Use industry-standard encryption to protect sensitive data in transit and at rest.
- B. Employ access control measures to limit who can view or alter critical data.
- C. Conduct regular vulnerability assessments and patch any system weaknesses.
- D. Provide security awareness training for all employees.



- E. Monitor our systems continuously to detect and respond to security incidents in real-time.

## **5. Privacy Risk Tolerance Statement**

My Small Business Inc. values the privacy of all individuals whose data we collect, process, and store. We have a zero-tolerance approach to privacy breaches and aim to comply with all applicable privacy laws and regulations, such as the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA).

We take the following measures to manage privacy risks:

- A. Minimize the collection and retention of personal data to what is strictly necessary.
- B. Implement data anonymization and pseudonymization techniques where possible.
- C. Ensure that third-party vendors handling our data follow the same rigorous privacy standards.
- D. Provide transparent information to clients and employees on how their data is used.
- E. Respond promptly to data subject access requests and privacy-related inquiries.

## **6. Risk Ownership**

Risk management is a collective responsibility at My Small Business Inc. The Risk Management Committee, led by senior management, is responsible for overseeing the implementation of risk management policies and ensuring compliance across the

organization. Department heads and individual employees also play an essential role in identifying and managing risks in their respective areas.

## **7. Continuous Improvement**

My Small Business Inc. is committed to continuous improvement in our risk management practices. This strategy will be reviewed and updated annually or as needed in response to emerging risks, changes in regulations, or business developments.

## **8. Conclusion**

Effective risk management is critical to the long-term success and sustainability of My Small Business Inc. We are committed to protecting our business, employees, and clients from risks, particularly in the areas of information security and privacy. By proactively managing risks, we aim to build trust, maintain compliance, and ensure operational resilience.

APPENDIX E:  
ASSET REGISTER TEMPLATE

<b>Asset ID</b>	Unique identifier for the asset ((E.g., A0001)
<b>Asset Type</b>	E.g., Laptop, Mobile, Website, Application
<b>Description</b>	Brief description of the risk (E.g., Dell XPS 13)
<b>Location</b>	E.g., Main Office, Employee Home
<b>Owner</b>	The person/department responsible for managing the asset
<b>Purchase Date</b>	E.g., 01-January-2024
<b>Condition</b>	E.g., Needs Replacement, Fair, Good, Excellent, N/A
<b>Value (USD)</b>	E.g., 1500
<b>Business Impact</b>	E.g., Critical, High, Medium, Low
<b>Disposal Date</b>	E.g., 01-January-2027
<b>Notes/Updates</b>	E.g., Updated OS on 01-September-2024

APPENDIX F:  
COMMON CONTROLS LIST

Control #	Control Category	Control Description	Baseline - Low	Baseline - Medium	Notes
CC-01	Access Control	Limit user access to critical systems and data based on roles and responsibilities.	Basic user permissions; administrative access to select individuals.	Role-based access control (RBAC) with periodic reviews of access rights.	Review access at least annually or after role changes.
CC-02	Multi-Factor Authentication (MFA)	Require additional verification (e.g., mobile, email) for system access.	Implement MFA for administrative access only.	Implement MFA for all users, particularly those accessing sensitive systems or data remotely.	Focus on protecting remote access points.
CC-03	Data Encryption	Encrypt sensitive data both in transit and at rest to prevent unauthorized access.	Encrypt data during transmission (e.g., SSL/TLS for websites).	Encrypt data both in transit and at rest, particularly for financial and customer information.	Ensure that key management processes are secure.
CC-04	Backups and Recovery	Regularly back up critical business data and ensure	Weekly backups of critical data; store backups off-	Daily backups with testing of restore procedures.	Test restore capabilities periodically

		the ability to recover from data loss.	site or in the cloud.	Maintain both local and off-site/cloud backups.	y (quarterly)
CC-05	Firewalls	Protect internal networks from unauthorized external access.	Basic firewall with default settings.	Advanced firewall with intrusion detection and prevention capabilities.	Regularly update firewall rules and monitor for suspicious activity.
CC-06	Antivirus/Antimalware	Implement antivirus and antimalware software on all devices.	Install basic antivirus software on all computers.	Use enterprise-grade antivirus software with automatic updates and periodic scans.	Configure the software for automatic updates and scanning.
CC-07	Incident Response Plan	Establish a plan to detect, respond to, and recover from security incidents.	Basic incident reporting procedure; maintain a list of contacts for incident reporting.	Documented incident response plan with defined roles and responsibilities. Perform post-incident reviews.	Review and update the plan annually or after any significant incident.
CC-08	Security Awareness Training	Educate employees on security best practices, including	Provide basic security training to all staff annually.	Implement a structured security awareness program with periodic	Update training materials as new threats emerge.

		phishing awareness.		phishing simulations.	
CC-09	Patch Management	Keep systems and software up to date to address known vulnerabilities.	Install security patches quarterly or when critical vulnerabilities are identified.	Automatic or scheduled patching process with monthly updates. Prioritize critical systems.	Ensure patch testing before deployment to avoid disruptions.
CC-10	Physical Security	Restrict physical access to sensitive areas and equipment.	Lock critical areas (e.g., server rooms) and restrict access to authorized personnel.	Implement badge access, video surveillance, and visitor logs for sensitive areas.	Review access logs monthly for any unusual activity.
CC-11	Third-Party Risk Management	Assess the security of vendors and partners who handle sensitive data.	Conduct basic assessments of vendors (e.g., security certifications, and reviews).	Formalize vendor agreements with clear security expectations and perform periodic audits.	Ensure that data-sharing agreements include security clauses.
CC-12	Password Management	Enforce strong password policies and the regular updating of passwords.	Minimum password complexity (e.g., 8 characters, mixed case). Require password changes every 6 months.	Enforce strong password policies (e.g., 12+ characters, no reuse). Use password managers for critical accounts.	Implement automatic password expiration and enforce complexity.

CC-13	Data Loss Prevention (DLP)	Prevent unauthorized access or sharing of sensitive data.	Basic DLP controls, such as disabling USB access on sensitive devices.	DLP software for monitoring and blocking unauthorized data transfers.	Review DLP logs for signs of data leakage.
CC-14	Logging and Monitoring	Log critical system events and monitor them for suspicious activity.	Enable basic logging on critical systems (e.g., server access logs).	Implement centralized logging with real-time monitoring and alerts for critical systems.	Review logs at least monthly, or after significant events.
CC-15	Business Continuity Planning	Prepare for business disruptions due to disasters or security incidents.	Maintain basic recovery procedures for critical operations (e.g., contact lists).	Develop a formal business continuity plan (BCP) with defined recovery objectives and timelines. Test BCP annually.	Regularly review BCP for updates to reflect changes in operations .
CC-16	Data Retention and Disposal	Establish policies for retaining and securely disposing of sensitive data.	Retain essential business records based on legal/regulatory requirements . Securely delete or destroy old data.	Implement comprehensive data retention schedules and use certified methods for secure data disposal (e.g., shredding, wiping).	Review and update retention policies annually.

APPENDIX G:  
INFORMATION TYPES LIST

<b>INF #</b>	<b>Information Type</b>	<b>Description</b>	<b>Risk Category</b>	<b>Example of Impact</b>	<b>Confidentiality Level</b>
INF-01	Personally Identifiable Information (PII)	Information that can identify an individual (e.g., name, SSN, address, phone number)	Privacy, Legal, Compliance	Data breach could lead to identity theft or legal penalties	High
INF-02	Financial Data	Financial records, including revenue, expense reports, invoices, credit card information	Financial, Compliance	Unauthorized access could result in fraud or financial loss	High
INF-03	Customer Information	Data related to customer orders, preferences, feedback, or contact information	Privacy, Operational	Loss or compromise could damage reputation and customer trust	Medium-High
INF-04	Employee Records	Internal HR information such as salaries, performance reviews, and health records	Privacy, Operational, Legal	Unauthorized disclosure could lead to employee dissatisfaction or legal action.	High
INF-05	Intellectual Property (IP)	Proprietary business information like trade secrets, patents,	Operational, Competitive	Loss of IP could harm business competitiveness or result in legal disputes.	High



		designs, or strategic plans			
INF-06	Contracts and Agreements	Legal documents related to business partnerships, clients, and suppliers	Legal, Operational	Breach of confidentiality could result in contract disputes or litigation	Medium-High
INF-07	Supplier Information	Data about suppliers, including contracts, pricing, and performance evaluations	Operational, Financial	Disruption could affect supply chain operations and lead to financial losses.	Medium
INF-08	Marketing Information	Data related to marketing strategies, campaign performance, and customer outreach	Operational, Competitive	Misuse could lead to competitive disadvantage or brand damage	Medium
INF-09	Sales and Revenue Data	Data related to sales performance, revenue forecasts, and customer orders	Financial, Operational	Inaccurate or lost data could affect business growth and financial planning.	Medium-High
INF-10	Business Continuity Plans	Plans for maintaining operations during disruptions, including disaster recovery plans	Operational, Strategic	Inadequate planning could result in extended downtime and revenue loss	High
INF-11	Software Source Code	Custom or proprietary software code developed by	Operational, Competitive	Loss or exposure could lead to intellectual	High

		the organization		property theft or security vulnerabilities.	
INF-12	Inventory Data	Data on stock levels, materials, and product availability	Operational, Financial	Inaccurate data could lead to supply shortages or excess inventory	Medium
INF-13	Incident Response Data	Logs and reports on past security breaches or incidents	Cybersecurity, Legal	Poor handling could lead to regulatory non-compliance and legal risks	High
INF-14	Health and Safety Records	Internal safety procedures, incident logs, and compliance reports	Legal, Operational	Non-compliance could lead to fines or operational shutdown	Medium
INF-15	Communication Records	Internal and external communication logs, including emails, memos, and meeting minutes	Legal, Operational	Disclosure could lead to legal issues or reputation damage	Medium
INF-16	Audit and Compliance Reports	Documents related to regulatory audits, internal reviews, and compliance with laws	Legal, Compliance	Inadequate reporting could lead to regulatory penalties or reputational harm.	High
INF-17	Research and Development (R&D) Data	Data related to product development, prototypes, or future business plans	Competitive, Strategic	A loss could compromise future growth or give competitors an advantage	High

INF-18	System Configuration Data	Information about IT systems, network configurations, and security settings	Cybersecurity, Operational	Exposure could lead to network vulnerabilities and system compromise	High
INF-19	Website Data	Data from website usage, analytics, and content management	Operational, Marketing	Downtime or data loss could impact customer experience and business performance.	Medium

APPENDIX H:  
RISK REGISTER TEMPLATE

**1. Risk Specifications**

<b>Risk ID</b>	Unique identifier for the risk (R0001)
<b>Risk Category</b>	E.g., Operational, Financial, Cybersecurity, Compliance
<b>Risk Description</b>	Brief description of the risk (e.g., data breach, supplier disruption)
<b>Date Identified</b>	Date when the risk was first identified
<b>Risk Owner</b>	The person/department responsible for managing the risk
<b>Likelihood (1-5)</b>	Probability of the risk occurring (1 = low, 5 = high)
<b>Impact (1-5)</b>	Impact of the risk on the organization (1 = low, 5 = high)
<b>Risk Level</b>	Overall risk level based on the likelihood and impact (e.g., High)
<b>Assessment Date</b>	Date the risk was assessed or updated.
<b>Assessor</b>	Name of the individual/team that performed the assessment
<b>Monitoring Frequency</b>	How often the risk is monitored (e.g., Monthly, Quarterly)
<b>Review Date</b>	Date of the last risk review
<b>Reviewer</b>	Name of the reviewer
<b>Notes/Updates</b>	Any updates or changes in the risk profile, status of mitigation actions, or new observations

**2. Controls Addressing the Risks**

<b>Control Measures</b>	<b>Mitigation Status</b>	<b>Control Owner</b>	<b>Due Date</b>
-------------------------	--------------------------	----------------------	-----------------

List of preventive or mitigating actions taken (e.g., install firewalls, diversify suppliers)	Status of the mitigation actions (e.g., (In Progress/Completed/Not Started)	The individual/team responsible for implementing the controls	The target date for completing the mitigation
---	---	---	---

APPENDIX I:  
INTERVIEW GUIDE TO ASSESS THE SUCCESS OF MCSF

**Introduction**

Note to Interviewer: As you've previously interacted with the participants through surveys and consultations, this interview guide builds upon that existing relationship. The goal is to evaluate the effectiveness of the minimalistic cybersecurity framework developed based on their feedback and needs.

**Section 1: Reflection on Previous Experiences**

1. Understanding of Previous Frameworks
  - a. How did you find the experience of learning NIST CSF and ISO 27001 during our earlier consultations?
  - b. What specific aspects of these frameworks did you find challenging or unmanageable?
2. Sustainability Concerns
  - a. You mentioned earlier that managing these frameworks without external help would be difficult. Could you elaborate on the factors contributing to this concern?
  - b. What support mechanisms do you think were lacking in the previous frameworks?
3. Impact on Business Operations

- a. How did the complexity of the previous frameworks affect your day-to-day business activities?
- b. Did they interfere with your primary focus on growth and operations?

## **Section 2: Initial Impressions of the Minimalistic Framework**

### 4. First Reactions

- a. What were your initial thoughts upon being introduced to the minimalistic cybersecurity framework?
- b. Did it seem more approachable compared to NIST CSF and ISO 27001?

### 5. Alignment with Needs

- a. Do you feel that this framework addresses the challenges you previously faced?
- b. How well does it align with your business priorities and resource limitations?

## **Section 3: Understanding and Clarity**

### 6. Language and Terminology

- a. Is the language used in the minimalistic framework clear and easy to understand?
- b. Were there any terms or concepts that remained unclear?

### 7. Guidance and Instructions

- a. Did the framework provide sufficient guidance for implementation?
- b. How does the clarity compare to that of NIST CSF and ISO 27001?

8. Ease of Comprehension

- a. Do you feel that someone without a cybersecurity background can grasp the framework effectively?
- b. What aspects contributed to making it easier or harder to understand?

**Section 4: Implementation Experience**

9. Adoption Process

- a. Have you started implementing the minimalistic framework in your organization?
- b. If yes, what steps have you taken so far?

10. Resource Requirements

- a. How did the resource needs (time, personnel, finances) for implementing this framework compare to previous ones?
- b. Was it manageable within your current capabilities?

11. Challenges Encountered

- a. What obstacles, if any, did you face during implementation?
- b. How did you overcome these challenges?

**Section 5: Effectiveness of Core Components**

12. Risk Identification and Prioritization

- a. How effective was the simplified risk identification process?
- b. Were you able to identify and prioritize risks specific to your business more easily?



13. Basic Protective Measures

- a. Have you implemented the recommended basic protective measures (e.g., software updates, strong passwords)?
- b. Do you find these measures practical and sustainable?

14. Incident Response Protocol

- a. Did you develop an incident response plan using the framework?
- b. Do you feel more prepared to handle potential cybersecurity incidents now?

**Section 6: Usability of Templates and Tools**

15. Risk Management Strategy Template

- a. Was the template helpful in formulating your risk management strategy?
- b. Did you need to modify it to suit your specific needs?

16. Asset Register Template

- a. Did the asset register assist you in cataloging and managing your assets?
- b. Is the process of maintaining the register straightforward?

17. Common Controls List

- a. Was the list of common controls useful in implementing security measures?
- b. Were the baseline levels (Low and Medium) appropriate for your organization?

18. Information Types Categorization

- a. Did the categorization of information types help in prioritizing data protection efforts?
- b. Was the confidentiality level assignment clear and beneficial?

#### 19. Risk Register Template

- a. Are you actively using the risk register to monitor and manage risks?
- b. Has it improved your risk management practices compared to before?

### **Section 7: Integration with Business Processes**

#### 20. Seamless Integration

- a. How easily did the framework integrate with your existing business operations?
- b. Did it require significant changes to your current workflows?

#### 21. Impact on Productivity

- a. Has implementing the framework affected your business productivity?
- b. Did it complement or compete with other business initiatives?

#### 22. Modularity and Flexibility

- a. Did the modular design allow you to implement components at your own pace?
- b. Are you planning to adopt additional modules as your business evolves?

### **Section 8: Independence and Sustainability**

#### 23. Managing Without External Help

- a. Do you feel confident in managing the framework independently moving forward?
- b. What factors contribute to your confidence or concerns in this area?

#### 24. Knowledge and Skills Development

- a. Has the framework helped improve your team's cybersecurity knowledge and skills?
- b. Do you feel better equipped to handle cybersecurity matters internally?

### **Section 9: Overall Satisfaction and Impact**

#### 25. Meeting Your Needs

- a. Does the minimalistic framework meet your organization's cybersecurity needs?
- b. How does it compare to your experiences with previous frameworks?

#### 26. Benefits Realized

- a. What are the most significant benefits you've observed since adopting the framework?
- b. Has there been an improvement in your cybersecurity posture and awareness?

#### 27. Return on Investment

- a. Do you believe the effort and resources invested in implementing the framework were worthwhile?
- b. Has it provided value in proportion to the costs involved?

## **Section 10: Suggestions and Future Improvements**

### 28. Areas for Enhancement

- a. Are there any aspects of the framework you think could be improved?
- b. What additional features or support would enhance its effectiveness for your business?

### 29. Unaddressed Challenges

- a. Are there any cybersecurity challenges you face that the framework did not address?
- b. How might these gaps be filled?

### 30. Recommendations to Others

- a. Would you recommend this framework to other small businesses or startups?
- b. What advice would you give to them based on your experience?

## **Section 11: Future Outlook**

### 31. Long-term Adoption

- a. Do you plan to continue using the minimalistic framework in the long term?
- b. How do you see it evolving with your business?

### 32. Ongoing Support Needs

- a. What kind of support would help you maintain and improve your cybersecurity practices?
- b. Are there resources or services you wish were available?

## **Conclusion**

Is there anything else you'd like to share about your experience with the minimalistic cybersecurity framework or if you have any additional comments/suggestions?

## REFERENCES

Abdulrasool, F.E. and Turnbull, S.J. (2020) “Exploring security, risk, and compliance-driven IT governance model for universities: applied research based on the COBIT framework.” *International Journal of Electronic Banking*, 2(3), pp.237-265.

Adriko, R. and Nurse, J.R. (2024) “Cybersecurity, cyber insurance, and small-to-medium-sized enterprises: a systematic review” *Information & Computer Security*, 32(5), pp.691-710.

Aggarwal, V.K. and Reddie, A.W. (2018) “Comparative industrial policy and cybersecurity: a framework for analysis”, *Journal of Cyber Policy*, 3(3), pp.291-305.

Agrawal, V. (2016) “Towards the Ontology of ISO/IEC 27005: 2011” *Risk Management Standard. In HAISA*, pp. 101-111.

Ajish, D. (2024) “Streamlining Cybersecurity: Unifying Platforms for Enhanced Defense”, *International Journal of Information Technology, Research and Applications*, 3(2), pp.48-57.

Aksoy, C. (2024) “Building a cyber security culture for resilient organizations against cyber attacks.” *İşletme Ekonomi ve Yönetim Araştırmaları Dergisi*, 7(1), pp.96-110.

Al-Ahmad, W. and Mohammad, B. (2013) “Addressing information security risks by adopting standards” *International Journal of Information Security Science*, 2(2), pp.28-43.

Al-Ahmad, W. and Mohammed, B.(2015) *A code of practice for effective information security risk management using COBIT 5*, Paper presented at the *Second International Conference on Information Security and Cyber Forensics (InfoSec)* November 2015, pp. 145-151. IEEE

Alahmari, A. and Duncan, B. (2020) Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. Paper presented at the 2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA), pp. 1-5. IEEE.

Alawadhi, M.W. and Awad, W.S.(2023) *Multi-Factor Authentication Modeling using Petri Nets*. Paper presented at the 2023 International Conference on IT Innovation and Knowledge Discovery (ITIKD) March 2023, pp. 1-5. IEEE.

Aldya, A.P., Sutikno, S. and Rosmansyah, Y.(2019) *Measuring the effectiveness of control of information security management system based on SNI ISO/IEC 27004: 2013 standard*. Paper presented at the Conference Series: Materials Science and Engineering. July 2019 (Vol. 550, No. 1, p. 012020). IOP Publishing.

Alexander, C.B. (2019) “The general data protection regulation and California consumer privacy act: The economic impact and future of data privacy regulations” *Loy. Consumer L. Rev.*, 32, p.199.

Almeida, R., Lourinho, R., da Silva, M.M. and Pereira, R. (2018) *A model for assessing COBIT 5 and ISO 27001 simultaneously*. Paper presented at the 2018 IEEE 20th Conference on Business Informatics July 2018 (CBI) (Vol. 1, pp. 60-69). IEEE.

Almuhammadi, S. and Alsaleh, M. (2017) “ Information security maturity model for NIST cyber security framework” *Computer Science & Information Technology (CS & IT)*, 7(3), pp.51-62.

Alshar'e, M. (2023) “Cyber security framework selection: Comparison of NIST and ISO27001” *Applied Computing Journal*, pp.245-255.

Alshboul, Y. and Streff, K. (2015) “Analyzing information security model for small-medium sized businesses”

Altaha, S. and Rahman, M.H.,(2023) *A mini literature review on integrating cybersecurity for business continuity*. Paper presented at the International Conference on Artificial Intelligence in Information and Communication February 2023 (ICAIIIC), pp. 353-359. IEEE.

Amoo, O.O., Atadoga, A., Osasona, F., Abrahams, T.O., Ayinla, B.S., and Farayola, O.A. (2024) “GDPR's impact on cybersecurity: A review focusing on USA and European practices” *International Journal of Science and Research Archive*, 11(1), pp.1338-1347.

Amore, E., Dilger, T., Ploder, C., Bernstein, R. and Mezzenzana, M. (2023) “Leverage the COBIT 2019 Design Toolkit in an SME Context: A Multiple Case Study” *KnE Social Sciences*, pp.73-101.

Andry, J.F. (2016) “Performance Measurement IT of Process Capability Model Based on COBIT: a Study Case.” *Data Manajemen dan Teknologi Informasi (DASI)*, 17(3), pp.21-26.

Anttila, J., Jussila, K., Kajava, J. and Kamaja, I. (2012) Integrating ISO/IEC 27001 and other managerial discipline standards with processes of management in organizations. Paper presented at the 2012 Seventh International Conference on Availability, Reliability and Security June 2012 (pp. 425-436). IEEE.

Anwar, M.J. and Gill, A. (2021) January. Developing an Integrated ISO 27701 and GDPR-based Information Privacy Compliance Requirements Model.” *In Australasian Conference on Information Systems 2020*.

Ariyani, S. and Sudarma, M. (2016) “Implementation Of The ISO/IEC 27005 In Risk Security Analysis Of Management Information System. “ *J. Eng. Res. Appl*, 6(8), pp.1-6.



Arogundade, O.R., “Strategic Security Risk Management in Cloud Computing: A Comprehensive Examination and Application of the Risk Management Framework.”

Asprion, P., Gossner, P. and Schneider, B.(2023) “Cybersecurity governance–An adapted practical framework for small enterprises”.

Azeem, M. (2021) “How Small Businesses can Adapt and Thrive In The Digital Economy: A Review of Best Practices.” *Business Review of Digital Revolution*, 1(1), pp.1-10.

Babenko, T., Hnatiienko, H. and Vialkova, V. (2020) “Modeling of the Integrated Quality Assessment System of the Information Security Management System.” *In IT&I Workshops*, pp. 75-84.

Baci, N., Vukatana, K. and Baci, M. (2022) “Machine learning approach for intrusion detection systems as a cyber security strategy for Small and Medium Enterprises.” *WSEAS Transactions on Business and Economics*, 19, pp.474-480.

Bada, M. and Nurse, J.R. (2019) “Developing cybersecurity education and awareness programs for small and medium-sized enterprises (SMEs). *Information & Computer Security*, 27(3), pp.393-410.

Bahuguna, A., Bisht, R.K. and Pande, J. (2018) Roadmap amid chaos: cyber security management for organizations. Paper presented at the 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT) July 2018 (pp. 1-6). IEEE.

Balisane, H., Egho-Promise, E.I., Lyada, E. and Aina, F. (2024) “TOWARDS IMPROVED THREAT MITIGATION IN DIGITAL ENVIRONMENTS: A COMPREHENSIVE FRAMEWORK FOR CYBERSECURITY ENHANCEMENT.” *International Journal of Research-GRANTHAALAYAH*, 12(5).

Ballou, B. and Heitger, D.L. (2005) “A building-block approach for implementing COSO's enterprise risk management-integrated framework.” *Management Accounting Quarterly*, 6(2), p.1.

Bar-Haim, R., Eden, L., Kantor, Y., Agarwal, V., Devereux, M., Gupta, N., Kumar, A., Orbach, M. and Zan, M. (2023) Towards Automated Assessment of Organizational Cybersecurity Posture in Cloud. Paper presented at the 6th Joint International Conference on Data Science & Management of Data (10th ACM IKDD CODS and 28th COMAD) pp. 167-175.

Barafort, B., Mesquida, A.L. and Mas, A. (2017) “ Integrating risk management in IT settings from ISO standards and management systems perspectives” *Computer Standards & Interfaces*, 54, pp.176-185.

Barnhill, B., 2023. Cyber Threat Data Sharing Practices Within the Federal Sector (Doctoral dissertation, Capella University).

Barrett, M., Barrett, M., Marron, J., Pillitteri, V.Y., Boyens, J., Quinn, S., Witte, G. and Feldman, L. (2020) *Approaches for federal agencies to use the cybersecurity framework*. Maryland, United States: US Department of Commerce, National Institute of Standards and Technology.

Bashofi, I. and Salman, M. ( 2022) *Cybersecurity maturity assessment design using NIST CSF, CIS CONTROLS v8 and ISO/IEC 27002*. Paper presented at the 2022 IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom) June 2022 pp. 58-62. IEEE.

Bashofi, I. and Salman, M. (2022) *Cybersecurity maturity assessment design using NIST CSF, CIS CONTROLS v8 and ISO/IEC 27002*. Paper presented at the IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom) June 2022 pp. 58-62. IEEE.

Baskaran, S.B.M., Arumugam, S. and Prasad, A.R. (2019) "Internet of Things security." *Journal of ICT Standardization*, 7(1), pp.21-42.

Batten, L. and Castleman, T. (2005) *Securing small business-the role of information technology policy*. ACIS 2005 p.79.

Ben-Israel, I. and Tabansky, L. (2011) "An interdisciplinary look at security challenges in the information age." *Military and Strategic Affairs*, 3(3), pp.21-37.

Benjamin, L.B., Adegbola, A.E., Amajuoyi, P., Adegbola, M.D. and Adeusi, K.B. (2024) "Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies." *Global Journal of Engineering and Technology Advances*, 19(2), pp.134-153.

Benz, M. and Chatterjee, D. (2020) "Calculated risk? A cybersecurity evaluation tool for SMEs" *Business Horizons*, 63(4), pp.531-540.

Berrada, H., Boutahar, J. and El Houssaïni, S.E.G. (2021) "Simplified IT risk management maturity audit system based on "COBIT 5 for Risk" *International Journal of Advanced Computer Science and Applications*, 12(8).

Berry, C.T. and Berry, R.L. (2018) "An initial assessment of small business risk management approaches for cyber security threats." *International Journal of Business Continuity and Risk Management*, 8(1), pp.1-10.

Beuran, R., Chinen, K.I., Tan, Y. and Shinoda, Y. (2016) Towards effective cybersecurity education and training.

Bhol, S.G., Mohanty, J.R. and Pattnaik, P.K.(2020) *Cyber security metrics evaluation using multi-criteria decision-making approach*. Paper presented at the Smart Intelligent Computing and Applications: Proceedings of the Third International Conference on Smart Computing and Informatics, Volume 2 (pp. 665-675). Springer Singapore.

Biega, A.J. and Finck, M.(2021) “Reviving purpose limitation and data minimization in data-driven systems.” *arXiv preprint arXiv:2101.06203*.

Blum, D. and Blum, D. (2020) “Establish a Control Baseline. Rational Cybersecurity for Business: The Security Leaders' Guide to Business Alignment”, pp.157-197.

Bodkhe, U., Tanwar, S., Parekh, K., Khanpara, P., Tyagi, S., Kumar, N. and Alazab, M. (2020) “Blockchain for industry 4.0: A comprehensive review.” *Ieee Access*, 8, pp.79764-79800.

Bollinger, J., Enright, B. and Valites, M. (2015) “Crafting the InfoSec playbook: security monitoring and incident response master plan.” *O'Reilly Media, Inc..*

Bounagui, Y., Hafiddi, H. and Mezrioui, A. (2016) “COBIT evaluation as a framework for cloud computing governance.” *International Journal of Cloud Applications and Computing (IJCAC)*, 6(4), pp.65-82.

Bradbard, D.A., Norris, D.R. and Kahai, P.H. (1990) “COMPUTER SECURITY IN SMALL BUSINESS: AN EMPIRICAL STUDY” *Journal of Small Business Management*, 28(1).

Brender, N. and Markov, I. (2013) “Risk perception and risk management in cloud computing: Results from a case study of Swiss companies.” *International journal of information management*, 33(5), pp.726-733.

Broad, J. (2013) “Risk Management Framework: A lab-based approach to securing Information Systems.” *Newnes*.

Brooks, S., Brooks, S., Garcia, M., Lefkovitz, N., Lightman, S. and Nadeau, E. (2017). “An introduction to privacy engineering and risk management in federal systems.”

Brown, J. (2024) “Strengthening digital safety for small businesses. *Computer Fraud & Security*”, 2024(3).

Burgess, S., Sellitto, C. and Karanasios, S. eds. (2009) “Effective web presence solutions for small businesses: Strategies for successful implementation: Strategies for successful implementation.” *IGI Global*.

Calder, A. and Watkins, S. (2019) “Information security risk management for ISO 27001/ISO 27002.” *It Governance Ltd*.

Calder, A.(2020) “Information Security based on ISO 27001/ISO 27002.” *Van Haren*.

Cartwright, A., Cartwright, E. and Edun, E.S. (2023) “Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies” *Computers & Security*, 131, p.103288.

Carvalho, C. and Marques, E., 2019, June. Adapting ISO 27001 to a public institution. In 2019 14th Iberian Conference on Information Systems and Technologies (CISTI), pp. 1-6. IEEE.

Cater-Steel, A., Tan, W.G. and Toleman, M., (2006) *Challenge of adopting multiple process improvement frameworks*. Paper presented at Proceedings of 14th European Conference on Information Systems (ECIS 2006).

Chaithanya, B.N. and Brahmananda, S.H. (2022) *Detecting ransomware attacks distribution through phishing urls using machine learning*. Paper presented at Computer Networks and Inventive Communication Technologies: Proceedings of Fourth ICCNCT 2021 (pp. 821-832). Springer Singapore.

Chandna, V. and Tiwari, P. (2023) “Cybersecurity and the new firm: surviving online threats.” *Journal of Business Strategy*, 44(1), pp.3-12.

Chaudhary, S., Gkioulos, V. and Katsikas, S. (2023) “A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises.” *Computer Science Review*, 50, p.100592.

Chidukwani, A., Zander, S. and Koutsakis, P. (2022) “A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations.” *IEEE Access*, 10, pp.85701-85719.

Christy, N.M.A., Baddam, P.R. and Amin, R. (2022) “Strategic approaches to safeguarding the digital future: insights into next-generation cybersecurity.” *Engineering International*, 10(2), pp.69-84.

Chittister, C.G. and Haimes, Y.Y. (1996) “Systems integration via software risk management.” *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, 26(5), pp.521-532.

Cissé, M. (2019) “Third-party risk management: Strategy to mitigate ‘on-premise and ‘cloud cyber security risks.” *Cyber Security: A Peer-Reviewed Journal*, 3(2), pp.103-115.

Coles-Kemp, L. and Overall, R.E. (2006) “The Information Security Ownership Question in ISO/IEC 27001”—*an Implementation*.

Collier, Z.A., DiMase, D., Walters, S., Tehranipoor, M.M., Lambert, J.H. and Linkov, I.(2014) “Cybersecurity standards: Managing risk and creating resilience. *Computer*”, 47(9), pp.70-76.

Cook, K.D.(2017) Effective cyber security strategies for small businesses.Doctoral dissertation, Walden University.

Coruh, U., Khan, M. and Bayat, O. (2021). *Lightweight offline authentication scheme for secure remote working environment*. Paper presented at the 2021 International Conference on Electrical, Computer, and Energy Technologies (ICECET), pp. 1-9. IEEE.

Crosier, A., McVey, D. and French, J. (2015) “By failing to prepare you are preparing to fail: lessons from the 2009 H1N1 ‘swine flu pandemic.” *The European Journal of Public Health*, 25(1), pp.135-139.

Crumpler, W. and Lewis, J.A., (2022) “Cybersecurity Workforce Gap ‘(p. 10). *Center for Strategic and International Studies (CSIS)*.

Cue, H.A.A., Bourlai, T. and Lupo, M. (2024) *A CIS Controls V8. 0 Scoring System using Combined Ranking-Weight Methods*. Paper presented at the 2024 IEEE International Systems Conference (SysCon), pp. 1-8. IEEE.

Cybersecurity, C.I. (2018) *Framework for improving critical infrastructure cybersecurity*. URL: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.4162018.p.7>.

D'Acquisto, G., Domingo-Ferrer, J., Kikiras, P., Torra, V., de Montjoye, Y.A. and Bourka, A.,(2015). *Privacy by design in big data: an overview of privacy-enhancing technologies in the era of big data analytics*. arXiv preprint arXiv:1512.06000.

Dalugama, M., “Cloud Computing: Detection and Prevention of DDoS Attacks Influencing the Adoption of Cloud Computing to the Small and Medium Enterprises in the Sri Lankan Business Context.”

Daniel, S.A. and Victor, S.S. (2024) “Emerging Trends in Cybersecurity for Critical Infrastructure Protection: A Comprehensive Review.” *Computer Science & IT Research Journal*, 5(3), pp.576-593.

Dedeke, A. (2017) “Cybersecurity framework adoption: using capability levels for implementation tiers and profiles.’ *IEEE Security & Privacy*, 15(5), pp.47-54.

Devos, J.(2007) “COBIT® “*Quickstart*.

Diamantopoulou, V., Tsohou, A. and Karyda, M. (2020) *From ISO/IEC 27002: 2013 information security controls to personal data protection controls: guidelines for GDPR compliance*. Paper presented at the Computer Security: ESORICS 2019 International Workshops, CyberICPS, SECPRE, SPOSE, and ADIoT, Luxembourg City,

Luxembourg, September 26–27, 2019 Revised Selected Papers 5 (pp. 238-257). Springer International Publishing.

Disterer, G. (2013) “ISO/IEC 27000, 27001 and 27002 for information security management” *Journal of Information Security*, 4(2).

Dkaidek, Z. and Rashid, A. (2024) “Bridging the Cybersecurity Skills Gap: Knowledge Framework Comparative Study.” *IEEE Security & Privacy*, 22(5), pp.88-95.

Dua, S., Shah, P. and AbdAllah, E.G.(2024) *Managing Third Party Risk for Small and Medium Enterprises*. Paper presented at the 2024 11th International Conference on Future Internet of Things and Cloud (FiCloud), pp. 209-214. IEEE.

Dutta, A. and Al-Shaer, E.(2019) “*what*”, “*where*”, and “*why*” *cybersecurity controls to enforce for optimal risk mitigation*. Paper presented at the 2019 IEEE Conference on Communications and Network Security (CNS) pp. 160-168. IEEE.

Ebrahim, T.Y. (2020) “National cybersecurity innovation” *W. Va. L. Rev.*, 123, p.483.

Ebuzor, J. ( 2024) “Understanding Customer Perception of Cyber Attacks: Impact on Trust and Security.” *In Corporate Cybersecurity in the Aviation, Tourism, and Hospitality Sector* pp. 83-111. IGI Global.

El-Gayar, O.F. and Fritz, B.D. (2010) “A web-based multi-perspective decision support system for information security planning.” *Decision Support Systems*, 50(1), pp.43-54.

Eloff, J.H., Labuschagne, L. and Badenhorst, K.P. (1993) “A comparative framework for risk analysis methods” *Computers & Security*, 12(6), pp.597-603.

ENTERPRISE, I.P.T.(2020) NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT, VERSION 1.0.



Erdogan, G., Halvorsrud, R., Boletsis, C., Tverdal, S. and Pickering, J.B., 2023. Cybersecurity awareness and capacities of SMEs.

Ernawati, T. and Nugroho, D.R.(2012) *IT risk management framework based on ISO 31000: 2009*. Paper presented at the International Conference on System Engineering and Technology (ICSET) September 2012 , pp. 1-8. IEEE.

Essentials, C., Brooks, F.E.C.J., Grow, C., Craig, P. and Short, D. (2018) *Local Network Security in the Real World*.

Fernandez De Arroyabe, I. and Fernandez de Arroyabe, J.C.(2023) “The severity and effects of Cyber-breaches in SMEs: a machine learning approach” *Enterprise Information Systems*, 17(3), p.1942997.

Ferrante, A.J.( 2018) “The impact of GDPR on WHOIS: Implications for businesses facing cybercrime” *Cyber Security: A Peer-Reviewed Journal*, 2(2), pp.143-148.

Fitroh, F., Seputra, M.R., Ramadhan, G., Hersyaf, T.N.H. and Rokhman, A.N., (2017). “Pentingnya Implementasi Iso 27001 Dalam Manajemen Keamanan: Sistematika Review.” *Prosiding Semnastek*.

Folorunso, A., Mohammed, V., Wada, I. and Samuel, B. ( 2024) “The impact of ISO security standards on enhancing cybersecurity posture in organizations” *World Journal of Advanced Research and Reviews*, 24(1), pp.2582-2595.

Force, J.T.(2017) “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy ”(Discussion Draft) (No. NIST Special Publication (SP) 800-37 Rev. 2 (Draft)). National Institute of Standards and Technology.

Force, J.T., (2017) *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (Discussion Draft)*

(No. NIST Special Publication (SP) 800-37 Rev. 2 (Draft)). National Institute of Standards and Technology.

Force, J.T.(2022) “Assessing security and privacy controls in information systems and organizations.” *NIST Special Publication, 800*, p.53A.

Fraccascia, L., Giannoccaro, I. and Albino, V. (2018) “Resilience of complex systems: State of the art and directions for future research.” *Complexity*, 2018(1), p.3421529.

Framework, C. (2021) Getting Started with the NIST.

Furnell, S., Heyburn, H., Whitehead, A. and Shah, J.N.(2020) “ Understanding the full cost of cyber security breaches” *Computer fraud & security*, 2020(12), pp.6-12.

Ganji, D., Kalloniatis, C., Mouratidis, H. and Gheytassi, S.M. (2019) “Approaches to develop and implement iso/iec 27001 standard-information security management systems: A systematic literature review.” *Int. J. Adv. Softw*, 12(3).

García-Porras, C., Huamani-Pastor, S. and Armas-Aguirre, J. (2018) *Information security risk management model for Peruvian SMEs*. Paper presented at the 2018 IEEE Sciences and Humanities International Research Conference (SHIRCON) 2018 (pp. 1-5). IEEE.

Ghanavati, S., Humphreys, L., Boella, G., Di Caro, L., Robaldo, L. and van der Torre, L.,(2014) *Compliance with multiple regulations*. Paper presented at the Conceptual Modeling: 33rd International Conference, ER 2014, Atlanta, GA, USA, October 27-29, 2014. (pp. 415-422). Springer International Publishing.

Gharajedaghi, J. (2011) “Systems thinking: Managing chaos and complexity: A platform for designing business architecture.” *Elsevier*.

Giuca, O., Popescu, T.M., Popescu, A.M., Prostean, G. and Popescu, D.E. ( 2021) A survey of cybersecurity risk management frameworks. Paper presented at the Soft

Computing Applications: Proceedings of the 8th International Workshop Soft Computing Applications (SOFA 2018), Vol. I 8, pp. 240-272. Springer International Publishing.

Gordon, L.A., Loeb, M.P. and Zhou, L. (2020) “Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model.” *Journal of Cybersecurity*, 6(1), p.tyaa005.

Gourisetti, S.N.G., Mylrea, M., Ashley, T., Kwon, R., Castleberry, J., Wright-Mockler, Q., McKenzie, P. and Brege, G. (2019) *Demonstration of the cybersecurity framework through real-world cyber attack*. Paper presented at the Resilience Week (RWS) July 2019 (Vol. 1, pp. 19-25). IEEE.

Govardhan, D., Krishna, G.G.S.H., Charan, V., Sai, S.V.A. and Chintala, R.R., (2023) *Key Challenges and Limitations of the OSINT Framework in the Context of Cybersecurity*. Paper at the 2023 2nd International Conference on Edge Computing and Applications July 2023 (ICECAA) , pp. 236-243. IEEE.

Griffy-Brown, C., Lazarikos, D. and Chun, M. (2019) “Emerging technologies and cyber risk: how do we secure the internet of things (IoT) environment?.” *Journal of Applied Business and Economics*, 21(2), pp.70-79.

Groš, S.,(2021) *A critical view on CIS controls*. Paper presented at the 2021 16th International Conference on Telecommunications (ConTEL) (pp. 122-128). IEEE.

Gupta, A. and Hammond, R. (2005) “Information systems security issues and decisions for small businesses: An empirical examination.” *Information management & computer security*, 13(4), pp.297-310.

Hanafi, R., Wibowo, L.A. and Rahayu, A. (2020). *Organization and IT strategic alignment, determination of IT process priorities using COBIT 5*. Paper presented at the International Conference on Advancement in Data Science, E-learning and Information Systems (ICADEIS) April 2020 pp. 1-6. IEEE.

Handayani, R., Utami, E. and Luthfi, E.T.(2023) “Systematic Literature Review on Auditing Information Technology Risk Management Using the COBIT Framework.” *Prisma Sains: Jurnal Pengkajian Ilmu dan Pembelajaran Matematika dan IPA IKIP Mataram*, 11(4), pp.1028-1036.

Harris, M., Patten, K., Regan, E. and Fjermestad, J.( 2012)Mobile and connected device security considerations: A dilemma for small and medium enterprise business mobility?.

Harris, M. and Patten, K.(2014) “Mobile device security considerations for small-and medium-sized enterprise business mobility.” *Information Management & Computer Security*, 22(1), pp.97-114.

Harrison, K. and White, G. (2012).*Information sharing requirements and framework needed for community cyber incident detection and response*. Paper presented at the IEEE Conference on Technologies for Homeland Security Nov 2012 (HST) (pp. 463-469). IEEE.

Härting, R.C., Kaim, R., Klamm, N. and Kroneberg, J. (2021) *Impacts of the New General Data Protection Regulation for small-and medium-sized enterprises*. Paper presented at the Fifth International Congress on Information and Communication Technology: ICICT 2020, London, Volume 1 ,2021 (pp. 238-246). Springer Singapore.

Hassani, H.L., Bahnasse, A., Martin, E., Roland, C., Bouattane, O. and Diouri, M.E.M. (2021) “Vulnerability and security risk assessment in a IIoT environment in compliance with standard IEC 62443.” *Procedia Computer Science*, 191, pp.33-40.

Hayden, L. (2009) “Designing common control frameworks: A model for evaluating information technology governance, risk, and compliance control rationalization strategies.” *Information Security Journal: A Global Perspective*, 18(6), pp.297-305.

Hayes, T., Tanner, M. and Schmidt, G. (2012) "Computer security threats: Small business professionals' confidence in their knowledge of common computer threats." *Advances in Business Research*, 3(1), pp.107-112.

Hazrati, M., Dara, R. and Kaur, J. (2022) "On-farm data security: practical recommendations for securing farm data." *Frontiers in Sustainable Food Systems*, 6, p.884187.

He, Y. and Janicke, H (2015) *Towards agile industrial control systems incident response*. Paper presented at 3rd International Symposium for ICS & SCADA Cyber Security Research 2015 (ICS-CSR 2015). BCS Learning & Developme.

Heidt, M. and Gerlach, J.P (2018) The influence of sme constraints on organizational IT Security.

Henriques, D., Pereira, R., Bianchi, I.S., Almeida, R. and Mira da Silva, M. (2020) "How IT Governance can assist IoT project implementation" *International Journal of Information Systems and Project Management*, 8(3), pp.25-45.

Hiller, J.S. and Russell, R.S. (2015) "Modalities for Cyber Security and Privacy Resilience: The NIST Approach." *In ISCRAM*.

Hiller, J.S. and Russell, R.S. (2017) "Privacy in crises: The NIST privacy framework" *Journal of Contingencies and Crisis Management*, 25(1), pp.31-38.

Ho, W., Zheng, T., Yildiz, H. and Talluri, S. (2015) "Supply chain risk management: a literature review" *International journal of production research*, 53(16), pp.5031-5069.

Hoy, Z. and Foley, A. (2015) "A structured approach to integrating audits to create organisational efficiencies: ISO 9001 and ISO 27001 audits." *Total Quality Management & Business Excellence*, 26(5-6), pp.690-702.

Hulitt, E. and Vaughn, R.B. (2010) “Information system security compliance to FISMA standard: a quantitative measure.” *Telecommunication Systems*, 45, pp.139-152.

Hutchings, A. (2012) “Computer security threats faced by small businesses in Australia.” *Trends and issues in crime and criminal justice*, (433), pp.1-6.

Hutchings, A., Smith, R.G. and James, L.(2013) “Cloud computing for small business: Criminal and security threats and prevention measures.” *Trends and issues in Crime and Criminal Justice*, (456), pp.1-8.

IBRAHIM, A. (2024) *Innovating Security: AI-Driven Solutions for Cyber Resilience*.

Ibrahim, A., Valli, C., McAteer, I. and Chaudhry, J. (2018) “A security review of local government using NIST CSF: a case study.” *The Journal of Supercomputing*, 74, pp.5171-5186.

Ilori, O., Nwosu, N.T. and Naiho, H.N.N. (2024) “A comprehensive review of it governance: effective implementation of COBIT and ITIL frameworks in financial institutions.” *Computer Science & IT Research Journal*, 5(6), pp.1391-1407.

Ilori, O., Nwosu, N.T. and Naiho, H.N.N.(2024). *Third-party vendor risks in IT security: A comprehensive audit review and mitigation strategies*.

Imsand, E., Tucker, B., Paxton, J. and Graves, S. (2020) “A survey of cyber security practices in small businesses. “*In National Cyber Summit (NCS) Research Track* (pp. 44-50). Springer International Publishing.

Isaca. ( 2013 ) *COBIT 5: Enabling information*. ISA.

Isaca. (2013) *Transforming Cybersecurity: Using COBIT 5*. ISA.

Isaca, (2014) *Implementing the NIST Cybersecurity Framework*. ISA.

Islam, M.T. and Karim, R. (2022) “Cybersecurity and Integrated Business Models. In *Integrated Business Models in the Digital Age: Principles and Practices of Technology Empowered Strategies* “(pp. 3-46). Cham: Springer International Publishing.

Itani, D., Itani, R., Eltweri, A.A., Faccia, A. and Wanganoo, L. (2024). *Enhancing Cybersecurity Through Compliance and Auditing: A Strategic Approach to Resilience*. Paper presented at the 2nd International Conference on Cyber Resilience (ICCR) february 2024 pp. 1-10. IEEE.

Jaeckels, T. and Yin, R. (2020) “Technology Business Management as a Driver of IT Governance, Risk, and Cybersecurity Improvement: A Case Study of Integrating TBM with COBIT Framework.” *International Journal of e-Education, e-Business, e-Management and e-Learning*, 10(1), pp.25-32.

Jang-Jaccard, J. and Nepal, S. (2014) “A survey of emerging threats in cybersecurity.” *Journal of computer and system sciences*, 80(5), pp.973-993.

Jauhari, M.A., Wardijono, B.A. and Hegarini, E. (2024) “Pengukuran Kematangan Keamanan Siber pada Perusahaan Teknologi Informasi dengan Framework Center for Internet Security Controls.” *Jurnal Saintekom: Sains, Teknologi, Komputer dan Manajemen*, 14(1), pp.72-83.

Jerbi, D. (2023) “Beyond Firewalls: Navigating the Jungle of Emerging Cybersecurity Trends.” *J Curr Trends Comp Sci Res*, 2(2), pp.191-195.

Johnson, B., Miller, M.S., Green, M.J.M., Arkady, M., Godin, M. and Nagy, B., (2022) “Game theory and prescriptive analytics for naval wargaming battle management aids.” *Technical Report, Naval Postgraduate School*.

.Joint Task Force Transformation Initiative, (2010) SP 800-37 Rev. 1. Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach. National Institute of Standards & Technology.

Juma, A.H., Arman, A.A. and Hidayat, F. (2023) *Cybersecurity Assessment Framework: A Systematic Review*. Paper presented at 10th International Conference on ICT for Smart Society (ICISS) 2023, pp. 1-6. IEEE.

Junior, A.S.C. and Arima, C.H. (2023) “Cyber risk management and iso 27005 applied in organizations: A systematic literature review.” *REVISTA FOCO*, 16(02), pp.e1188-e1188.

Junior, C.R., Becker, I. and Johnson, S. (2023) *Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity*. arXiv preprint arXiv:2309.17186.

Kabanda, S., Tanner, M. and Kent, C.(2018) “Exploring SME cybersecurity practices in developing countries.” *Journal of Organizational Computing and Electronic Commerce*, 28(3), pp.269-282.

Kandpal, S., Bhatt, S., Mohan, L., Patwal, A. and Kumar, P. (2023) *Cyber Security Implementation Issues in Small to Medium-sized Enterprises (SMEs) and their Potential Solutions: A Comprehensive Analysis*. Paper presented at the 14th International Conference on Computing Communication and Networking Technologies (ICCCNT) ,July 2023 , pp. 1-5. IEEE.

Kapoor, K., Renaud, K. and Archibald, J. (2018 ) *Preparing for GDPR: helping EU SMEs to manage data breaches*. In 2018 AISB Convention: Symposium on Digital Behaviour Intervention for Cyber Security.

KARAGOZLU, D., AJAMU, J. and MBOMBO, A.B.(2020) “Adaptation and effects of cloud computing on small businesses. “ *Brain. Broad research in artificial intelligence and neuroscience*, 11(4), pp.149-167.

Khaleefah, A.D. and Al-Mashhadi, H.M.(2024) “Methodologies, Requirements, and Challenges of Cybersecurity Frameworks: A Review.” *Iraqi Journal of Science*.



Khanagha, S., Volberda, H. and Oshri, I. (2014) “Business model renewal and ambidexterity: structural alteration and strategy formation process during transition to a Cloud business model.” *R&D Management*, 44(3), pp.322-340.

Kim, J.J. and Hong, S.P.(2011) “A method of risk assessment for multi-factor authentication.” *Journal of Information Processing Systems*, 7(1), pp.187-198.

Kirsch, L. and Boss, S. (2007) “The last line of defense: motivating employees to follow corporate security guidelines.” *ICIS 2007 proceedings*, p.103.

Kissoon, T. (2020) “Optimum spending on cybersecurity measures.” *Transforming Government: People, Process and Policy*, 14(3), pp.417-431.

Klien, A. and Mohamed, A. (2022) “Cybersecurity Intrusion Detection for Station and Process Bus Applications in Substations: Challenges and Experiences.” *In 2022 Saudi Arabia Smart Grid (SASG)*, pp. 1-5. IEEE.

Knauer, C. (2019) “How contact centres can leave businesses exposed to cybercrime.” *Network Security*, 2019(11), pp.6-9.

Kohnke, A., Sigler, K. and Shoemaker, D. (2016) “Strategic risk management using the NIST risk management framework.” *EDPACS*, 53(5), pp.1-6.

Kurii, Y. and Opirskyy, I., (2022) “Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001: 2013.” *NIST Spec. Publ*, 800(53), p.10.

Kwon, J. and Eric, J.M.(2011) “The Impact of Security Practices on Regulatory Compliance and Security Performance.” *In ICIS*.

La Rovere, R.L., Antônio Pedro da Costa e Silva Lima<sup>1</sup> Guilherme de Oliveira Santos<sup>2</sup> Pedro Paulo Cardoso Barcellos Ferreira<sup>3</sup>.

Lachow, I.(2011)“The Stuxnet enigma: Implications for the future of cybersecurity.” *Georgetown Journal of International Affairs*, pp.118-126.

Lackey, R.(2013) “E-commerce systems security for small businesses.” *International Journal of Network Security & Its Applications*, 5(2), p.193.

Landis, C.B. and Kroll, J.A. (2024) Mitigating Inference Risks with the NIST Privacy Framework. Proceedings on Privacy Enhancing Technologies.”

Latifi, F. and Zarrabi, H. (2017) “A COBIT5 Framework for IoT risk management.” *International Journal of Computer Applications*, 170(8), pp.40-43.

Leasa, Z.V. and Prassida, G.F.(2024) “Manajemen Risiko pada Sistem Informasi Akademik Universitas XYZ menggunakan ISO 27005: 2018.” *Jurnal Teknologi Dan Sistem Informasi Bisnis*, 6(4), pp.649-656.

Lee, Y. and Larsen, K.R.(2009) “Threat or coping appraisal: determinants of SMB executives’ decision to adopt anti-malware software.” *European Journal of Information Systems*, 18(2), pp.177-187.

Lin, W.C. and Saebeler, D.(2019) “Risk-Based V. Compliance-Based Utility Cybersecurity-a False Dichotomy.” *Energy LJ*, 40, p.243.

Liou, J.J., Chuang, Y.C., Zavadskas, E.K. and Tzeng, G.H (2019) “Data-driven hybrid multiple attribute decision-making model for green supplier evaluation and performance improvement.” *Journal of Cleaner Production*, 241, p.118321.

Llanten-Lucio, Y.I., Amador-Donado, S. and Márceles-Villalba, K. (2022) “Validation of cybersecurity framework for threat mitigation.” *Revista Facultad de Ingeniería*, 31(62).

Lloyd, G.( 2020) “The business benefits of cyber security for SMEs.” *Computer fraud & security*, 2020(2), pp.14-17.

Longras, A., Pereira, T., Carneiro, P. and Pinto, P.(2018) *On the track of ISO/IEC 27001: 2013 implementation difficulties in Portuguese organizations*. Paper presented at

the 2018 International Conference on Intelligent Systems (IS) ,June 2018 ,pp. 886-890. IEEE.

Lopes, I.M., Guarda, T. and Oliveira, P. (2019) *How ISO 27001 can help achieve GDPR compliance*. Presented at the 14th Iberian Conference on Information Systems and Technologies (CISTI) June 2019 , pp. 1-6, IEEE.

Lopes, I.M., Guarda, T. and Oliveira, P. (2019) “Implementation of ISO 27001 standards as GDPR compliance facilitator.” *Journal of information systems engineering & management*, 4(2), pp.1-8.

Lubell, J., Lubell, A. and Lubell, J. (2016) “Baseline Tailor User Guide. US Department of Commerce,” *National Institute of Standards and Technology*.

Madnick, S., Marotta, A., Novaes Neto, N. and Powers, K. (2019) Research Plan to Analyze the Role of Compliance in Influencing Cybersecurity in Organizations. Available at SSRN 3567388.

Mäkkä, K. and Kampová, K. (2024) “Cyber Security and Business Continuity Management: Ensuring Resilience in a Digital World” *Challenges to National Defence in Contemporary Geopolitical Situation*, 1(1).

Makridis, C.A.(2021) “Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018.” *Journal of Cybersecurity*, 7(1), p.tyab021.

Malatji, M., (2023) *Management of enterprise cyber security: A review of ISO/IEC 27001: 2022*. Paper presented at International conference on cyber management and engineering (CyMaEn) January 2023 , pp. 117-122. IEEE.

Maleh, Y. and Maleh, Y.(2022) *Cybersecurity in Morocco*. Springer.

Manda, J.K.(2020) *Cloud Security Best Practices for Telecom Providers: Developing comprehensive cloud security frameworks and best practices for telecom*

service delivery and operations, drawing on your cloud security expertise. Available at SSRN 5003526.

Mangalaraj, G., Singh, A. and Taneja, A., 2014, August. IT Governance Frameworks and COBIT-A Literature Review. In AMCIS.

Marican, M.N.Y., Othman, S.H., Selamat, A. and Abd Razak, S., 2023. Quantifying the Return of Security Investments for Technology Startups. *Baghdad Science Journal*.

Martelo, R.J., Madera, J.E. and Betín, A.D. (2015) “Software para gestión documental, un componente modular del Sistema de Gestión de Seguridad de la Información (SGSI).” *Información tecnológica*, 26(2), pp.129-134.

Mavridis, I.P., Androulakis, A.I., Halkias, A.B. and Mylonas, P., 2011, September. Real-life paradigms of wireless network security attacks. In 2011 15th Panhellenic Conference on Informatics pp. 112-116, IEEE.

Mayer, J. and Fagundes, L.L (2009) *A model to assess the maturity level of the risk management process in information security*. Paper presented at IFIP/IEEE International Symposium on Integrated Network Management-Workshops, June 2009 pp. 61-70, IEEE.

Mijnhardt, F., Baars, T. and Spruit, M.(2016) “Organizational characteristics influencing SME information security maturity.” *Journal of Computer Information Systems*, 56(2), pp.106-115.

MILITARU, P.C. and COSTIN, D., Human Resources Security Management towards ISO/IEC 27001: 2005 accreditation of an Information Security Management System.

Mitchell, R.B. and Jones, T.(2002) “Policies controlling use of computer-based resources in small businesses.” *Journal of Computer Information Systems*, 42(4), pp.77-83.

Mittal, A., Pandian, P.K.G., Kaur, J., Prasad, N. and Devaguptapu, B., (2023) “*Innovative Security Frameworks For Iot And Cloud Computing Integration: Challenges And Solutions.*” *Webology* (ISSN: 1735-188X), 20(3).

Mmango, N. and Gundu, T.(2023) *Cyber Resilience in the Entrepreneurial Environment: A Framework for Enhancing Cybersecurity Awareness in SMEs.* Paper presented at 2023 International Conference on Electrical, Computer and Energy Technologies (ICECET),November 2023 , pp. 1-6 , IEEE.

Mohammed, D. (2015) “Cybersecurity compliance in the financial sector” *Journal of Internet Banking and Commerce*, 20(1), pp.1-11.

Mohammed, D., Omar, M. and Nguyen, V. (2017) “Enhancing Cyber Security for Financial Industry through Compliance and Regulatory Standards.” *In Security Solutions for Hyperconnectivity and the Internet of Things*,pp. 113-129, IGI Global.

Mohd Ludin, W.N.E.W. and Mohd, M.(2024) “Comparative Analysis of Small and Medium-Sized Enterprises Cybersecurity Program Assessment Model” *International Journal of Advanced Computer Science & Applications*, 15(8).

Moneva, A. and Leukfeldt, R.(2023) “Insider threats among Dutch SMEs: Nature and extent of incidents, and cyber security measures.” *Journal of Criminology*, 56(4), pp.416-440.

Montenegro, C. and Moncayo, D.(2016) “Information Security Risk in SMEs: A Hybrid Model Compatible with IFRS. In de 2016 6th International Conference on Information Communication and Management.

Moore, T., Dynes, S. and Chang, F.R.(2016) “Identifying how firms manage cybersecurity investment” *In Workshop on the Economics of Information Security (WEIS)* ,pp. 1-27.

Morimoto, S.,(2009 *Application of COBIT to security management in information systems development*. Paper presented at the 2009 Fourth International Conference on Frontier of Computer Science and Technology,December 2009 , pp. 625-630, IEEE.

Morrisson, M.K.(2020) “Best practice models for enterprise resource planning implementation and security challenges.” *Journal of Business*, 8(2), pp.55-60.

Moudoubah, L., El Yamami, A., Mansouri, K. and Qbadou, M.(2021) “From IT service management to IT service governance: An ontological approach for integrated use of ITIL and COBIT frameworks.” *International Journal of Electrical and Computer Engineering*, 11(6), p.5292.

Mudau, E., Mathonsi, T.E. and Tshilongamulenzhe, T. (2024) *A Deep Learning Algorithm to Minimize Cyber-Security Attacks for Small Enterprises*. Paper presented at the 2024 International Conference on Electrical, Computer and Energy Technologies ICECET, July 2024 , pp. 1-7, IEEE.

Muhammad, A.H., Santoso, J.D. and Akbar, A.F.I.(2023) “Information security investment prioritization using best-worst method for small and medium enterprises.” *Indonesian Journal of Electrical Engineering and Computer Science*, 31(1), pp.271-280.

Mylrea, M., Gourisetti, S.N.G. and Nicholls, A. (2017) “An introduction to buildings cybersecurity framework” *In 2017 IEEE symposium series on computational intelligence (SSCI)* (pp. 1-7). IEEE.

Ncubukezi, T. (2024) June. Risk Assessment for Malware Attacks in Small Businesses. *In European Conference on Cyber Warfare and Security* (Vol. 23, No. 1, pp. 305-312).

Nicho, M. and Muumaar, S. (2016) “Towards a taxonomy of challenges in an integrated IT governance framework implementation.” *Journal of International Technology and Information Management*, 25(2), p.2.

Nykanen, R. and Karckainen, T.(2014) “Aligning two specifications for controlling information security” *International Journal of Cyber Warfare and Terrorism (IJCWT)*, 4(2), pp.46-62.

Ofori-Yeboah, A., Addo-Quaye, R., Oseni, W., Amarin, P. and Agangmikre, C., (2021) “ Cyber supply chain security: a cost benefit analysis using net present value” *In 2021 International Conference on Cyber Security and Internet of Things (ICSIoT)* pp. 49-54. IEEE.

Ogbanufe, O., Kim, D. and Takabi, H.(2016) “Top Manager's Perspectives on Cyberinsurance Risk Management for Reducing Cybersecurity Risks.” *In AMCIS* pp. 20-43.

Ogunyebi, O., Swar, B. and Aghili, S. (2018) “ An Incident Handling Guide for Small Organizations in the Hospitality Sector.” *In Trends and Advances in Information Systems and Technologies: Volume 1* 6 pp. 232-241. Springer International Publishing.

Olaniyan, J. and Ogunola, A.A.(2024) “Protecting small businesses from social engineering attacks in the digital era” *World J Adv Res Rev*, 24(03), pp.834-53.

Omar, M. (2015) “Insider threats: Detecting and controlling malicious insiders.” *In New Threats and Countermeasures in Digital Crime and Cyber Terrorism* pp. 162-172. IGI Global.

Ometov, A., Bezzateev, S., Makitalo, N., Andreev, S., Mikkonen, T. and Koucheryavy, Y. (2018) “Multi-factor authentication: A survey. *Cryptography*”, 2(1), p.1.

Onwubiko, C. and Onwubiko, A.(2019) “Cyber KPI for return on security investment.” *In 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)* pp. 1-8. IEEE.

Pacheco, J., Tunc, C. and Hariri, S.(2018) Security framework for IoT cloud services.Paper presented at *IEEE/ACS 15th International Conference on Computer Systems and Applications* ,2018 (AICCSA) pp. 1-6. IEEE.

PANAOUSIS, E., Cyber Risk Assessment and Optimization: A Small Business Case Study.

Parmar, M. and Miles, A.(2024) “Cyber Security Frameworks (CSFs): An Assessment Between the NIST CSF v2. 0 and EU Standards.” *In 2024 Security for Space Systems (3S)* pp. 1-7. IEEE.

Parsons, J., 1996. An information model based on classification theory. *Management Science*, 42(10), pp.1437-1453.

Paté-Cornell, M.E., Kuypers, M., Smith, M. and Keller, P. (2018) “Cyber risk management for critical infrastructure: a risk analysis model and three case studies.” *Risk Analysis*, 38(2), pp.226-241.

Patiño, S., Solís, E.F., Yoo, S.G. and Arroyo, R. (2018) *ICT risk management methodology proposal for governmental entities based on ISO/IEC 27005*.Paper presented at the International Conference on eDemocracy & eGovernment (ICEDEG),2018 pp. 75-82. IEEE.

Patterson, J.(2017) Cyber-security policy decisions in small businesses. Doctoral dissertation, Walden University.

Paulsen, C. and Toth, P.(2016) Small business information security: The fundamentals (No. NIST Internal or Interagency Report (NISTIR) 7621 Rev. 1). National Institute of Standards and Technology.

Paulsen, C. (2016 ) Cybersecuring small businesses. *Computer*, 49(8), pp.92-97.



Pawar, S. and Palivela, H., (2022) “LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs).” *International Journal of Information Management Data Insights*, 2(1), p.100080.

Phillips, R. and Tanner, B.,(2019) “Breaking down silos between business continuity and cyber security.” *Journal of business continuity & emergency planning*, 12(3), pp.224-232.

Phirke, A. and Ghorpade-Aher, J.(2019) “Best practices of auditing in an organization using ISO 27001 standard.” *Int. J. Recent Technol. Eng*, 8(2), pp.691-695.

Pickering, B., Phillips, S.C. and Erdogan, G.(2023) *I Just Want to Help: SMEs Engaging with Cybersecurity Technology*. *International Conference on Human-Computer Interaction*, July 2023 pp. 338-352. Cham: Springer Nature Switzerland.

Ponsard, C. and Grandclaudon, J.(2019) *Guidelines and tool support for building a cybersecurity awareness program for smes*. Paper presented at the International Conference on Information Systems Security and Privacy, February 2019 pp. 335-357. Cham: Springer International Publishing.

Ponsard, C., Grandclaudon, J. and Bal, S.(2019) “Survey and Lessons Learned on Raising SME Awareness about Cybersecurity.” *ICISSP*, pp.558-563.

Proença, D. and Borbinha, J. (2018) *Information security management systems-a maturity model based on ISO/IEC 27001*. Paper presented at the Business Information Systems: 21st International Conference, BIS 2018, Berlin, Germany, July 18-20, 2018, pp. 102-114. Springer International Publishing.

Putra, A.P. and Soewito, B. (2023) “Integrated Methodology for Information Security Risk Management using ISO 27005: 2018 and NIST SP 800-30 for Insurance Sector.” *International Journal of Advanced Computer Science and Applications*, 14(4).

Putra, S.J., Gunawan, M.N., Sobri, A.F., Muslimin, J.M. and Saepudin, D.(2020) *Information Security Risk Management Analysis Using ISO 27005: 2011 For The Telecommunication Company*. Paper presented at the 8th International Conference on Cyber and IT Service Management (CITSM),October 2020, pp. 1-5. IEEE.

Raineri, E.M. and Resig, J. (2020) “Evaluating self-efficacy pertaining to cybersecurity for small businesses” *Journal of Applied Business and Economics*, 22(12).

Rayhan, A., *Cybersecurity in the Digital Age: Assessing Threats and Strengthening Defenses*.

Rea-Guaman, M., Calvo-Manzano, J.A. and San Feliu, T.(2018) A prototype to manage cybersecurity in small companies. Paper presented at 13th Iberian Conference on Information Systems and Technologies (CISTI).June 2018 pp. 1-6. IEEE.

Renvall, A.(2018) Improving cybersecurity through ISO/IEC 27001 information security standard in the context of SMEs.

Ridley, G., Young, J. and Carroll, P. (2004). *COBIT and its Utilization: A framework from the literature*. Paper presented at 37th Annual Hawaii International Conference on System Sciences, 2004 pp. 8. IEEE.

Roberts, S.A. (2021) “Exploring the Relationships Between User Cybersecurity Knowledge, Cybersecurity and Cybercrime Attitudes, and Online Risky Behaviors.” Northcentral University.

Rohn, E., Sabari, G. and Leshem, G. (2016) “Explaining small business InfoSec posture using social theories.” *Information & Computer Security*, 24(5), pp.534-556.

Romanosky, S. (2016) “Examining the costs and causes of cyber incidents.” *Journal of Cybersecurity*, 2(2), pp.121-135.

Ross, R., Katzke, S. and Toth, P.(2005) “ The new FISMA standards and guidelines changing the dynamic of information security for the federal government” In MILCOM 2005-2005 IEEE Military Communications Conference ,pp. 864-870. IEEE.

Ross, R., Katzke, S. and Toth, P. (2005). “The new FISMA standards and guidelines changing the dynamic of information security for the federal government. In MILCOM 2005-2005 IEEE Military Communications Conference (pp. 864-870). IEEE.

Ross, R.A.(2023) The ongoing threat of ransomware to small businesses: A qualitative case study on the impediments to the application of preventative, detective, and corrective controls. Doctoral dissertation, Northcentral University.

Ross, R.S. and Johnson, L.A.(2010) “Guide for applying the risk management framework to federal information systems: A security life cycle approach.”

Ross, R.S., (2018) “Risk management framework for information systems and organizations: A system life cycle approach for security and privacy.”

Roy, P.P.(2020) A high-level comparison between the nist cyber security framework and the iso 27001 information security standard. Paper presented at 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTE),February 2020 pp. 1-3. IEEE.

Rusman, A., Nadlifatin, R. and Subriadi, A.P.(2022) “Information system audit using COBIT and ITIL framework: literature review.” *Sinkron: jurnal dan penelitian teknik informatika*, 6(3), pp.799-810.

Ryan, J.J.C.H.(2000) “Information security practices and experiences in small businesses.” The George Washington University.

Sadeghi, A.R., Wachsmann, C. and Waidner, M. (2015) *Security and privacy challenges in industrial internet of things*. Paper presented at the 52nd annual design automation conference,June 2015 , pp. 1-6.

Saha, B. and Anwar, Z.(2024) “A Review of Cybersecurity Challenges in Small Business: The Imperative for a Future Governance Framework.” *Journal of Information Security*, 15(01), pp.24-39.

Salvi, H.U. and Surve, S.S. (2023) “Emerging trends and future prospects of cybersecurity technologies: addressing challenges and opportunities.” *International Journal of Scientific Research in Science and Technology*, 5(23), p.10432.

Sandhu, R.S. (1998) “Role-based access control.” *In Advances in computers* (Vol. 46, pp. 237-286). Elsevier.

Sangani, N.K. and Vijayakumar, B. (2012) “Cyber security scenarios and control for small and medium enterprises.” *Informatica Economica*, 16(2), p.58.

Saritac, U., Liu, X. and Wang, R. (2022) *Assessment of cybersecurity framework in critical infrastructures*. Paper presented at IEEE Delhi Section Conference (DELCON) (pp. 1-4), February 2010,IEEE.

Sawant, P. and Kpmg, I.(2020) “ Holistic approach to information security risk management.” *Int J Eng Res Technol (IJERT)*, 9(7), pp.42-44.

Schlarman, S. (2007) “Selecting an IT control framework. EDPAC: The EDP Audit, Control, and Security Newsletter, 35(2), pp.11-17.

Selznick, L.F. and LaMacchia, C.(2017) “Cybersecurity liability: How technically savvy can we expect small business owners to be.” *J. Bus. & Tech. L.*, 13, p.217.

Shackelford, S.J., Russell, S. and Haut, J. (2015) “Bottoms up: A comparison of voluntary cybersecurity frameworks.’ *UC Davis Bus. LJ*, 16, p.217.

Shackelford, S.J., Russell, S. and Haut, J. (2015) “Bottoms up: A comparison of voluntary cybersecurity frameworks.” *UC Davis Bus. LJ*, 16, p.217.

Shameli-Sendi, A., Shajari, M., Hassanabadi, M., Jabbarifar, M. and Dagenais, M., (2012) "Fuzzy multi-criteria decision-making for information security risk assessment" *The Open Cybernetics & Systemics Journal*, 6(1).

Sharma, A., "THE IMPACT OF CYBERSECURITY BREACHES ON BIG BUSINESSES." *International Journal of Advanced Research*, 12(10).

Sheikhpour, R. and Modiri, N.,(2012) "An approach to map COBIT processes to ISO/IEC 27001 information security management controls." *International Journal of Security and Its Applications*, 6(2), pp.13-28.

Shelly, M. and Jackson, M. (2009) "Doing business with consumers online: Privacy, security and the law." *International Journal of Law and Information Technology*, 17(2), pp.180-205.

Shen, L.,(2014) "The NIST cybersecurity framework: Overview and potential impacts." *Scitech Lawyer*, 10(4), p.16.

Siponen, M.T.(2001) "An analysis of the recent IS security development approaches: descriptive and prescriptive implications." *In Information security management: global challenges in the new millennium* (pp. 101-124). IGI Global.

Skrodelis, H.K., Strebko, J. and Romanovs, A. (2020) *The information system security governance tasks in small and medium enterprises*. Paper presented at 61st International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS), 2020, pp. 1-4. IEEE.

Slonka, K.J., (2020) "MANAGING CYBER SECURITY COMPLIANCE ACROSS BUSINESS SECTORS". *Issues in Information Systems*, 21(1).

Smith, J.B., Smith, C.G., Kietzmann, J. and Lord Ferguson, S.T.(2022) "Understanding micro-level resilience enactment of everyday entrepreneurs under threat." *Journal of Small Business Management*, 60(5), pp.1202-1245.

Steenkamp, G. (2011) "The applicability of using COBIT as a framework to achieve compliance with the King III Report's requirements for good IT governance." *Southern African Journal of Accountability and Auditing Research*, 11(1), pp.1-8.

Stone, R. (2016) "Fraud, security, and controls in small businesses: A proposed research agenda." *Journal of Business*, 1(3), pp.15-21.

Subhani, A., Khan, I.A. and Zubair, A.(2021) "Review of insider and insider threat detection in the organizations." *Journal of Advanced Research in Social Sciences and Humanities*, 6(4), pp.167-174.

Sujatha, G.(2024) "System Hardening using CIS Benchmarks. In 2024 International Conference on Advances in Computing" *Communication and Applied Informatics (ACCAI)* (pp. 1-6). IEEE.

Sukumar, A., Mahdiraji, H.A. and Jafari-Sadeghi, V. (2023) "Cyber risk assessment in small and medium-sized enterprises".

Sulistyowati, D., Handayani, F. and Suryanto, Y. (2020) "Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss." *JOIV: International Journal on Informatics Visualization*, 4(4), pp.225-230.

Suryawan, A.D. (2018) *Information technology service performance management using COBIT and ITIL frameworks: A case study*. Paper presented at International Conference on Information Management and Technology (ICIMTech), 2018 (pp. 223-228). IEEE.

Sussy, B., Wilber, C., Milagros, L. and Carlos, M. (2015). *ISO/IEC 27001 implementation in public organizations: A case study*. Paper presented at the 10th Iberian conference on information systems and technologies (CISTI) ,June 2010 (pp. 1-6). IEEE.

Tam, T., Rao, A. and Hall, J. (2021) "The good, the bad and the missing: A Narrative review of cyber-security implications for Australian small businesses." *Computers & Security*, 109, p.102385.

Tanner, N.H. (2019) *Cybersecurity Blue Team Toolkit*, Wiley ISBN:9781119552949

Tariq, M.I., Haq, D. and Iqbal, J.A.V.E.E.D. (2013) "SLA based information security metric for cloud computing from COBIT 4.1 framework." *International Journal of Computer Networks and Communications Security*, 1(3), pp.95-101.

Tene, O. and Polonetsky, J. (2012) "Big data for all: Privacy and user control in the age of analytics." *Nw. J. Tech. & Intell. Prop.*, 11, p.239.

Teymourlouei, H. and Harris, V. (2019) *Effective methods to monitor IT infrastructure security for small business*. Presented at the International Conference on Computational Science and Computational Intelligence (CSCI), 2019, pp. 7-13. IEEE.

Thapa, C. and Camtepe, S.(2021) "Precision health data: Requirements, challenges and existing techniques for data security and privacy." *Computers in biology and medicine*, 129, p.104130.

Thomas, D.M., Sanghvi, A., Touhiduzzaman, M.D., Wand, P. and Reynolds, T., (2022) "Guide to the Distributed Energy Resource Risk Management Framework (No. NREL/TP-5R00-81715)." *National Renewable Energy Lab.(NREL), Golden, CO (United States)*.

Thong, J.Y., Yap, C.S. and Raman, K.S. (1994) "Engagement of external expertise in information systems implementation." *Journal of Management Information Systems*, 11(2), pp.209-231.

Thong, J.Y., Yap, C.S. and Raman, K.S.(1996) “ Top management support, external expertise and information systems implementation in small businesses.” *Information systems research* 7(2), pp.248-267.

Tsiodra, M., Panda, S., Chronopoulos, M. and Panaousis, E.(2023) “Cyber risk assessment and optimization: A small business case study.” *IEEE Access*, 11, pp.44467-44481.

Tupkalo, V., Cherepkov, S. and Yarmolatii, A. (2024) *A systematic process-oriented approach to the implementation of the enterprise's information security management system. Measurements infrastructure*, (8).

Ugbebor, F., Aina, O., Abass, M. and Kushanu, D. (2024) “EMPLOYEE CYBERSECURITY AWARENESS TRAINING PROGRAMS CUSTOMIZED FOR SME CONTEXTS TO REDUCE HUMAN-ERROR RELATED SECURITY INCIDENTS.” *Journal of Knowledge Learning and Science Technology* ISSN: 2959-6386 (online), 3(3), pp.382-409.

Unuakhalu, M.F., Sigdel, D. and Garikapati, M.(2014) “Integrating risk management in system development life cycle.” *International Journal of Software and Web Sciences (IJSWS)*, 8(1), pp.1-9.

Utomo, D., Wijaya, M., Suzanna, S., Efendi, E. and Sagala, N.T.M.(2022). “Leveraging COBIT 2019 to Implement IT Governance in SME Context: A Case Study of Higher Education in Campus A.” *CommIT (Communication and Information Technology) Journal*, 16(2), pp.129-141.

Valdevit, T., Mayer, N. and Barafort, B. (2009) *Tailoring ISO/IEC 27001 for SMEs: a guide to implement an information security management system in small settings*. Paper presented at Software Process Improvement: 16th European Conference, EuroSPI 2009, Alcala (Madrid), Spain, September 2009, pp. 201-212. Springer Berlin Heidelberg.



Van Haastrecht, M., Sarhan, I., Shojaifar, A., Baumgartner, L., Mallouli, W. and Spruit, M. (2021) A threat-based cybersecurity risk assessment approach addressing SME needs. Paper presented at the 16th International Conference on Availability, Reliability and Security, August 2021, pp. 1-12.

Veerasingam, P., Abd Razak, S., Abidin, A.F.A., Mohamed, M.A. and Satar, S.D.M., (2023) "INTRUSION DETECTION AND PREVENTION SYSTEM IN SME'S LOCAL NETWORK BY USING SURICATA." *Malaysian Journal of Computing and Applied Mathematics*, 6(1), pp.21-30.

Vidgen, R., Henneberg, S. and Naudé, P.(2007) "What sort of community is the European Conference on Information Systems? A social network analysis 1993–2005." *European Journal of Information Systems*, 16(1), pp.5-19.

von Solms, R.(1997) *Can security baselines replace risk analysis?. In Information Security in Research and Business*. Paper presented at the IFIP TC11 13th international conference on Information Security (SEC'97),14–16 May 1997, Copenhagen, Denmark, pp. 91-98. Springer US.

Vorster, A. and Labuschagne, L.E.S. (2005) *A framework for comparing different information security risk analysis methodologies*. Paper presented at Annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries ,July 2005 ,pp. 95-103.

Waiganjo, I., Osakwe, J. and Azeta, A. (2024) "Impediments to Cybersecurity Policy Implementation in Organisations: Case Study of Windhoek, Namibia." *International Journal of Research and Scientific Innovation*, 11(10), pp.540-546.

Wallace, S., Green, K.Y., Johnson, C., Cooper, J. and Gilstrap, C.(2020) "An extended TOE framework for cybersecurity-adoption decisions." *Communications of the Association for Information Systems*, 47(1), p.51.

Wang, C.H. and Tsai, D.R.(2009) *Integrated installing ISO 9000 and ISO 27000 management systems on an organization*. Paper presented at the 43rd Annual 2009 international carnahan conference on security technology, October 2009,

Wang, W., Sadjadi, S.M. and Rishe, N. (2024) *A Survey of Major Cybersecurity Compliance Frameworks*. Paper presented at 2024 IEEE 10th Conference on Big Data Security on Cloud (BigDataSecurity), May 2024 , IEEE.

Wangen, G., Hallstensen, C. and Snekenes, E.(2018) “A framework for estimating information security risk assessment method completeness: Core Unified Risk Framework, CURF.” *International Journal of Information Security*, 17.

Warren, M.J., Rd, B. and Burwood, M., FOSTERING INFORMATION SECURITY CULTURE IN SMALL AND MEDIUM SIZE ENTERPRISES.

Weng, Y. and Wu, J. (2024)”Leveraging artificial intelligence to enhance data security and combat cyber attacks.”*Journal of Artificial Intelligence General science (JAIGS)* 5(1) pp.3006-4023.Available at <https://ojs.boulibrary.com/index.php/JAIGS/article/view/211> Accessed (31<sup>st</sup> December 2024)

Werlinger, R., Hawkey, K. and Beznosov, K. (2009) “An integrated view of human, organizational, and technological challenges of IT security management.” *Information Management & Computer Security*, 17(1), pp.4-19.

White, G.B. and Sjelin, N. (2022) “The NIST cybersecurity framework.” *In Research Anthology on Business Aspects of Cybersecurity* (pp. 39-55). IGI Global.

Whitman, M. (2018) *Challenges in the Instruction of Risk Management*.

Wijaya, A.(2023) “Penyelarasan Tujuan dan Sasaran Bisnis Teknologi Informasi Menggunakan Kerangka Kerja COBIT 4.1.” *JuSiTik: Jurnal Sistem dan Teknologi Informasi Komunikasi*, 7(1), pp.1-6.

Wilkinson, G.(2018) “General data protection regulation: No silver bullet for small and medium-sized enterprises.” *Journal of Payments Strategy & Systems*, 12(2), pp.139-149.

Williams, P.A. and Manheke, R.J. (2010) *Small business-a cyber resilience vulnerability*.

Wilson, M., McDonald, S., Button, D. and McGarry, K.(2023) “It won’t happen to me: surveying SME attitudes to cyber-security”.*Journal of Computer Information Systems*, 63(2), pp.397-409.

Witzke, E.L. (2015) *Selecting RMF controls for national security systems (No. SAND2015-6770)*. Sandia National Lab. (SNL-NM), Albuquerque, NM (United States).

Wolff, J. and Lehr, W. (2017) Degrees of ignorance about the costs of data breaches: What policymakers can and can't do about the lack of good empirical data. Available at SSRN 2943867. Accessed (31<sup>st</sup> December 2024).

Xie, N. and Mead, N.R. (2004) *SQUARE project: cost/benefit analysis framework for information security improvement projects in small companies*.

Yeboah-Boateng, E.O. (2013) “Of Social Engineers & Corporate Espionage Agents: How Prepared Are SMEs in Developing Economies?” *Journal of Electronics & Communications Engineering Research*, 1(3), pp.14-22.

Yildirim, E.Y., Akalp, G., Aytac, S. and Bayram, N. (2011) “Factors influencing information security management in small-and medium-sized enterprises: A case study from Turkey.” *International Journal of Information Management*, 31(4), pp.360-365.

Yudhiyati, R., Putritama, A. and Rahmawati, D.(2021) “What small businesses in developing country think of cybersecurity risks in the digital age: Indonesian case.” *Journal of Information, Communication and Ethics in Society*, 19(4), pp.446-462.

Zeinolabedin, N., Mehrvarz, S.A. and Rahbar, N. (2014) *How COBIT Can Complement ITIL TO Achieve BIT*. arXiv preprint arXiv:1407.2379.

Zhang, X., Wuwong, N., Li, H. and Zhang, X. (2010) *Information security risk management framework for the cloud computing environments*. Paper presented on 10th IEEE international conference on computer and information technology ,2010 (pp. 1328-1334). IEEE.

Zhou, M., Zhang, R., Xie, W., Qian, W. and Zhou, A. (2010) *Security and privacy in cloud computing: A survey*. Paper presented on 2010 sixth international conference on semantics, knowledge and grids , November 2010 (pp. 105-112). IEEE.

Zolotarev, V., Oleynikova, A. and Zakhir, B. (2024) *Dynamic Playbooks Quality Metrics*. Paper presented at the conference on 2024 International Russian Smart Industry Conference (SmartIndustryCon), March 2024, (pp. 249-254). IEEE.

Zulkifli, M.S., Hassan, N.H., Maarop, N., Rahim, F.A. and Anuar, M.S.M.(2023) *A Proposed Multifactor Authentication Framework for SME in Cloud Computing Environment*. Paper presented at the 2023 IEEE 13th International Conference on System Engineering and Technology (ICSET) (pp. 307-312). IEEE.