



KADIR HAS UNIVERSITY
SCHOOL OF GRADUATE STUDIES
PROGRAM OF MANAGEMENT INFORMATION SYSTEMS

**CYBER RESILIENCE ABILITY CONTROL
ASSESSMENT ON A RISK CENTRIC AND PERSONA
BASED ZTNA APPROACH**

YAPRAK KURTLUTEPE

MASTER OF SCIENCE THESIS

ISTANBUL, JULY, 2023

Yaprak Kurtlutepe

Master of Science Thesis

2023

CYBER RESILIENCE ABILITY CONTROL ASSESSMENT ON A RISK CENTRIC AND PERSONA BASED ZTNA APPROACH

YAPRAK KURTLUTEPE

ADVISOR: PROF. DR. HASAN DAĞ

A thesis submitted to
the School of Graduate Studies of Kadir Has University
in partial fulfilment of the requirements for the degree of
Master of Science in Management Information Systems

Istanbul, July, 2023

APPROVAL

This thesis titled CYBER RESILIENCE ABILITY CONTROL ASSESSMENT ON A RISK CENTRIC AND PERSONA BASED ZTNA APPROACH submitted by YAPRAK KURTLUTEPE, in partial fulfillment of the requirements for the degree of Master of Science in Management Information Systems is approved by

Prof. Dr. Hasan Dağ (Advisor)
Kadir Has University

.....

Prof. Dr. Mustafa Bağrıyanık
Istanbul Technical University

.....

Assoc. Prof. Dr. Mehmet Nafiz Aydın
Kadir Has University

.....

I confirm that the signatures above belong to the aforementioned faculty members.

Prof. Dr. Mehmet Timur Aydemir
Director of the School of Graduate Studies
Date of Approval: 21.07.2023

DECLARATION ON RESEARCH ETHICS AND PUBLISHING METHODS

I, YAPRAK KURTLUTEPE; hereby declare

- that this Master of Science Thesis that I have submitted is entirely my own work and I have cited and referenced all material and results that are not my own in accordance with the rules;
- that this Master of Science does not contain any material from any research submitted or accepted to obtain a degree or diploma at another educational institution;
- and that I commit and undertake to follow the "Kadir Has University Academic Codes of Conduct" prepared in accordance with the "Higher Education Council Codes of Conduct".

In addition, I acknowledge that any claim of irregularity that may arise in relation to this work will result in a disciplinary action in accordance with the university legislation.

Yaprak Kurtlutepe

Date: 21.07.2023

ACKNOWLEDGEMENT

Firstly, I want to say a big thank you to my advisor, Prof. Dr. Hasan Dağ; your guidance has been crucial in making this thesis possible, and your support has been invaluable.

I must also thank my father, Ahmet Kurtlutepe. In all the difficulties I encountered during my thesis writing process, he first supported me, made the stressful times easier for me, and always had full faith in me. He always encouraged me to be successful in academia. Thanks to his efforts, I was able to write this thesis. I appreciate everything you've done to help me.

A special thanks to my friends Lidya, Hayal, Nihal, and Stefani. Your friendship made the hard times easier and the process a lot more enjoyable. You were by my side every time I felt like I was losing my joy and creativity. I would like to thank each and every one of you for all the emotional and spiritual energy you have provided during this process. I will never forget your presence during those times.

I want to acknowledge my manager, Alen, and all my teammates. Your understanding and support during this period have meant a lot to me.

I appreciate everyone who has helped me during this time. Whether your contribution was big or small, it has been essential to the completion of this thesis. Your guidance and encouragement have been invaluable, and I am truly grateful for the time and effort you have invested in me. I am confident that the knowledge and skills I have gained through this experience will continue to benefit me in my future endeavours.

CYBER RESILIENCE ABILITY CONTROL ASSESSMENT ON A RISK CENTRIC AND PERSONA BASED ZTNA APPROACH

ABSTRACT

This thesis embarks on an in-depth exploration of cyber resilience in organizations of varying sizes through the application of an innovative, dual-pronged auditing approach via introducing cyber resilience as a measurable metric for organizations for the first time. In an era marked by a rapidly evolving cyber landscape, understanding and enhancing cyber resilience has become paramount. The central instrument to achieve this is the 'Risk-Based and Persona Based Cyber Resiliency Assessment Kit'. It incorporates both risk-based and persona-based evaluations to offer a comprehensive and adaptive evaluation of an organization's cybersecurity posture. The research meticulously applies this dual-audit approach across five diverse organizations, spanning from a large-sized multinational company to a small start-up, with a medium-sized organization, an SME, and a university included in between. The dual-scoring system, which yields a risk-based audit score along with a persona-based audit score, provides a granular and precise understanding of cyber resilience prevalent amongst the participant organizations. Via underscoring the significance of adopting a comprehensive, context-sensitive, and strategic approach to cybersecurity measures. The findings demonstrate that the degree of cyber resilience is not directly proportionate to the size of an organization. While the research acknowledges certain limitations, such as the sample size and the reliance on self-reported data, it also identifies potential areas for future exploration. This includes the integration of advanced data analytics and machine learning in cybersecurity, understanding the impact of organizational factors on cyber resilience, and the development of industry-specific audit methodologies. In essence, the thesis presents a holistic view of cyber resilience, offering key insights and recommendations for enhancing cyber resilience strategies within organizations, irrespective of their size or sector.

Keywords: cyber security, cyber resilience, zero-trust, assessment kit, cybersecurity posture, information technology standards, cyber security standards, information security

RİSK ODAKLI VE KİŞİ TABANLI ZTNA YAKLAŞIMINDA SİBER DAYANIKLILIK YETENEK KONTROLÜ DEĞERLENDİRMESİ

ÖZET

Bu tez, siber dayanıklılığı ilk kez kuruluşlar için ölçülebilir bir metrik olarak sunarak, yenilikçi, çift yönlü bir denetim yaklaşımının uygulanması yoluyla farklı boyutlardaki kuruluşlarda siber dayanıklılığın derinlemesine araştırılmasını önermektedir. Hızla gelişen bir siber dünyanın revaçta olduğu bir çağda, siber dayanıklılığı anlamak ve geliştirmek çok önemli hale gelmiştir. Bunu başarmanın temel aracı olarak ‘Risk Bazlı ve Persona Bazlı Siber Dayanıklılık Değerlendirme Seti’ bu tezde sunulmuştur. Bu setler, bir kuruluşun siber güvenlik duruşunun kapsamlı ve uyarlanabilir bir değerlendirmesini sunmak için hem risk tabanlı hem de kişi tabanlı değerlendirmeleri birleştirir. Araştırma, bu ikili denetim yaklaşımını, büyük ölçekli çok uluslu bir organizasyondan küçük bir start-up'a, orta ölçekli bir kuruluşa, bir KOBİ'ye ve bir üniversiteye kadar uzanan beş farklı kuruluşa titizlikle uyguluyor. Kişiyeye dayalı bir denetim puanıyla birlikte riske dayalı bir denetim puanı veren ikili puanlama sistemi, katılımcı kuruluşlar arasında yaygın olan siber direncin ayrıntılı ve net bir şekilde anlaşılmasını, siber güvenlik önlemlerine kapsamlı, bağlama duyarlı ve stratejik bir yaklaşım benimsemesinin önemini vurgulamaktadır. Bulgular, siber dayanıklılık derecesinin bir kuruluşun büyüklüğü ile doğrudan orantılı olmadığını göstermektedir. Araştırma, örneklem büyüklüğü ve kişisel olarak bildirilen verilere dayanma gibi belirli sınırlamaları kabul etse de, gelecekteki keşifler için potansiyel alanları da tanımlar. Bu, gelişmiş veri analitiği ve makine öğreniminin siber güvenliğe entegrasyonunu, kurumsal faktörlerin siber dayanıklılık üzerindeki etkisinin anlaşılmasını ve sektöre özel denetim metodolojilerinin geliştirilmesini içerir. Özünde bu tez, siber dayanıklılığa bütüncül bir bakış açısı sunarak, büyüklükleri veya sektörleri ne olursa olsun kuruluşlar içinde siber dayanıklılık stratejilerini geliştirmek için önemli içgörüler ve öneriler sunuyor.

Anahtar Sözcükler: siber güvenlik, siber dayanıklılık, sıfır güven, değerlendirme seti, siber güvenlik duruşu, bilgi teknolojileri standartları, siber güvenlik standartları, bilgi güvenliği

TABLE OF CONTENTS

ACKNOWLEDGEMENT	V
ABSTRACT.....	VI
ÖZET	VII
1. INTRODUCTION	1
1.1 BACKGROUND AND CONTEXT OF CYBERSECURITY AND CYBER RESILIENCY	1
1.2 OBJECTIVES AND SCOPE OF THE THESIS	14
1.3 OVERVIEW OF THE METHODOLOGY	19
2. LITERATURE REVIEW	22
2.1 BRIEF HISTORY OF THE INTERNET.....	22
2.2 BRIEF HISTORY OF CYBERSECURITY.....	26
2.3 CYBERSECURITY CONCEPTS, DEFINITIONS, AND RELATED TERMINOLOGY	29
2.4 EXISTING APPROACHES FOR MEASURING CYBER RESILIENCY.....	36
2.4.1 <i>The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)</i>	<i>36</i>
2.4.2 <i>Factor Analysis of Information Risk (FAIR).....</i>	<i>36</i>
2.4.3 <i>The Center for Internet Security (CIS) Critical Security Controls</i>	<i>37</i>
2.4.4 <i>NIST Special Publication (SP) 800-53</i>	<i>37</i>
2.4.5 <i>NIST SP 800-160 Vol. 2</i>	<i>38</i>
2.4.6 <i>The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)</i>	<i>38</i>
2.5 ZERO TRUST PHILOSOPHY AND ITS RELEVANCE TO CYBER RESILIENCY.....	39
2.5.1 <i>Applying maritime warfare insights: zero-trust, multi-factor authentication, and cyber resiliency in the digital age - a case study from the HMAS Sydney-Kormoran encounter.....</i>	<i>39</i>
2.6 ZERO TRUST PHILOSOPHY	44
2.7 LITERATURE GAPS.....	45
3. METHODOLOGY	49
3.1 DESCRIPTION AND DEVELOPMENT OF CYBER RESILIENCY CONTROL MATRICES.....	49

3.2 RESEARCH DESIGN	51
3.3 ETHICAL CONSIDERATIONS	51
3.4 AUDIT QUESTIONS AND THEIR REFERENCES	52
3.5 RISK-BASED CYBER RESILIENCY ASSESSMENT KIT	55
3.5.1 Control's Risk Score (CRS):	57
3.5.2 Number of Audit Questions (naq)	59
3.5.3 Maximum Risk Score of the Organization (MRSO)	59
3.5.4 Control-Based Risk Score (CBRS)	59
3.5.5 Organisation's Actual Risk Score (OARS)	60
3.5.6 Organisations Risk-Based Cyber Resiliency Score (RB):	61
3.6 PERSONA-BASED ZERO-TRUST RESILIENCY ASSESSMENT KIT	61
3.6.1 Number of Persona (np)	63
3.6.2 Number of Audit Questions (naq)	63
3.6.3 Value of Zero-trust (VZT)	63
3.6.4 Number of "Yes" Answers (nya)	64
3.6.5 Persona-Based Score (PBS)	64
3.6.6 Calculation of the Score of Persona-Based Assessment Result (PB)	64
3.7 TOTAL CYBER RESILIENCY SCORE OF THE ORGANIZATION	64
4. RESULTS AND ANALYSIS	65
4.1 CASE STUDIES: APPLICATION OF THE CYBER RESILIENCY ABILITY CONTROL ASSESSMENTS	65
4.1.1 Overview of the Assessed Organizations	65
4.1.1.1 Large-sized organisation	66
4.1.1.2 Medium-sized organisation	67
4.1.1.3 SME	68
4.1.1.4 Small-sized organisation	69
4.1.1.5 University	70
5. DISCUSSION	72
5.1 SUMMARY OF THE MAIN FINDINGS	72
5.2 IMPLICATIONS OF THE RESEARCH FOR ORGANIZATIONS AND CYBERSECURITY PRACTITIONERS	73
5.3 LIMITATIONS OF THE STUDY AND POTENTIAL AREAS FOR FUTURE RESEARCH	74
6. CONCLUSION	77

BIBLIOGRAPHY.....	79
APPENDIX A.....	85
A.1 SAMPLE OF VOLUNTARY PARTICIPATION CONSENT FORM	85
VOLUNTARY PARTICIPATION CONSENT FORM.....	85
APPENDIX B.....	86
B.1 SAMPLE OF RISK-BASED ASSESSMENT KIT	86
<i>B.1.1 One Sample Ability Control Question for Each Ability Section.....</i>	<i>86</i>
<i>B.1.2 Sample Risk Analysis Section for Risk-Based Assessment Kit</i>	<i>121</i>
B.2 QUESTION POOL FOR THE RISK-BASED ASSESSMENT KIT	122
APPENDIX C.....	156
C.1 SAMPLE OF PERSONA-BASED ASSESSMENT KIT	156
C.2 ABILITY CONTROL QUESTIONS WITH THEIR IDS FOR THE PERSONA-BASED ASSESSMENT KIT	157
C.3 ABILITY CONTROL QUESTIONS' REFERENCES	159
<i>PB-CR.1</i>	<i>159</i>
<i>PB-CR.2</i>	<i>160</i>
<i>PB-CR.3</i>	<i>160</i>
<i>PB-CR.4</i>	<i>161</i>
<i>PB-CR.5</i>	<i>161</i>
<i>PB-CR.6</i>	<i>162</i>
<i>PB-CR.7</i>	<i>163</i>
<i>PB-CR.8</i>	<i>163</i>
<i>PB-CR.9</i>	<i>163</i>
<i>PB-CR.10</i>	<i>164</i>
<i>PB-CR.11</i>	<i>165</i>
<i>PB-CR.12</i>	<i>166</i>
<i>PB-CR.13</i>	<i>166</i>
<i>PB-CR.14</i>	<i>167</i>
<i>PB-CR.15</i>	<i>168</i>
<i>PB-CR.16</i>	<i>170</i>
<i>PB-CR.17</i>	<i>171</i>
<i>PB-CR.18</i>	<i>172</i>
<i>PB-CR.19</i>	<i>174</i>

<i>PB-CR.20</i>	175
<i>PB-CR.21</i>	176
<i>PB-CR.22</i>	177
<i>PB-CR.23</i>	178
<i>PB-CR.24</i>	179
<i>PB-CR.25</i>	179
<i>PB-CR.26</i>	180
<i>PB-CR.27</i>	181
APPENDIX D	183
D.1 SAMPLE AUDIT REPORT.....	183
AUDIT RESULTS	183
CONCLUSION AND RECOMMENDATIONS	184



1. INTRODUCTION

1.1 Background and Context of Cybersecurity and Cyber Resiliency

The ever-evolving nature of cybersecurity threats has created a continuing challenge for enterprises and governments in the rapidly expanding field of information technology. Significant advancements in artificial intelligence and machine learning are driving this expansion. Since the beginning of computer networks, adversaries have sought to disrupt, damage, or gain unauthorised access to sensitive information by exploiting vulnerabilities and breaching security measures. The objective is to gain unauthorised access to sensitive data. This constant conflict between defenders and attackers has impacted the development of practices and regulations about cybersecurity.

Throughout cybersecurity's history, the most frequently encountered threats have been computer viruses and worms, whose primary goals have been to replicate themselves and disrupt systems. In 1988, for instance, there was an outbreak of a computer virus known as the Morris Worm, which quickly swept across the early stages of the internet and affected thousands of machines (Spafford, 1989). This incident highlighted the potential for harm to be caused using cyber methods and paved the way for further investigation and advancement in cybersecurity.

The internet became increasingly valuable to our day-to-day lives as technology improved. As a result, the level of complexity of cyber threats increased along with it. The evolution of malicious software may be broken down into five distinct phases (Alenezi et al., 2020), with ransomware being recognised as a particularly pernicious group version. It is possible to trace the origin of ransomware back to the first boot sector viruses, such as Stoned and a variation called Monkey. Joseph L. Popp's invention of the AIDS Trojan in 1989 was a crucial turning point in the history of ransomware (Bansal, 2021). The increasing number of newly developed ransomware variants throughout 2011 highlights the growing threat these malicious apps pose and the urgent need for effective defences. Ransomware is becoming more complex, as seen by the increase in novel

variations throughout the past twelve months (Alenezi et al., 2020). Notable ransomware attacks, such as WannaCry and NotPetya in 2017, caused substantial damage across various industries, including healthcare, transportation, and telecommunications (Bansal, 2021).

The hazards that accompany cybersecurity have been reinforced in recent years by advanced persistent threats (APTs) and state-sponsored cyberwarfare (Kumar et al., 2022). APTs, distinguished by their continuous and discrete nature, cause tremendous ongoing harm to organisations that are their targets. The 2010 attack, Stuxnet, which targeted Iran's nuclear facilities and caused significant operational losses, is a leading instance of the remarkable capabilities of advanced distinctive threats (Kumar et al., 2022). State-sponsored cyber warfare has also become an important concern, with occurrences such as the 2014 breach of Sony Pictures (Kim et al., 2020) and the 2016 hack of the Democratic National Committee (Tran, 2018) emphasising the possible geopolitical repercussions of cyber assaults.

The progression of cyber threats over time, from simple computer viruses and worms in the past to more current and advanced attacks in the present, highlights the dynamic difficulties associated with information security. Also, by looking at key events throughout the history of cybersecurity and their impact on organisations and governments, the importance of maintaining a solid cybersecurity stance and the need for continuous research and development in this area remain up-to-date. This foundation is essential for accurately predicting and responding to future challenges in the rapidly evolving field of cybersecurity.

Organisations have increasingly relied on information technology and interconnected networks in the digital age to conduct operations, deliver services, and maintain a competitive edge (Constantinides, Henfridsson, and Parker 2018). The transition is motivated by various significant elements (Nambisan, Wright, and Feldman 2019), such as the prevalence of potent and economical computing gadgets (Volkodaeva, Balanovskaya, and Rustenova 2022), the extensive accessibility of high-speed internet connectivity (Amankwah-Amoah et al. 2021), and the increasing necessity for enterprises

to exploit vast data quantities for examination and strategic determinations (Nambisan, Wright, and Feldman 2019). Organisations have implemented various technologies, including cloud computing, artificial intelligence, and the Internet of Things (IoT), to optimise efficiency, simplify procedures, and provide novel solutions to satisfy customer demands (Urbach and Röglinger 2019). Moreover, the worldwide integration of business and the necessity for efficient teamwork among individuals in different regions have resulted in the implementation of advanced communication and collaboration technologies (Amankwah-Amoah et al. 2021). And, of course, in addition to that, The global COVID-19 pandemic has expedited the process of digitisation for organisations worldwide. This has resulted in the need to implement sophisticated communication and collaboration technologies to enable effective remote work and ensure the uninterrupted operation of businesses. The heightened awareness of the amplified risks associated with an expanded digital presence has resulted in a corresponding increase in the need for resilient cybersecurity protocols. While advantageous, the augmented dependence on technology also poses a greater susceptibility to cyber threats (Lallie et al. 2021), thereby mandating the implementation of strong cybersecurity protocols to safeguard confidential data and ensure uninterrupted business operations. As a result, the current cybersecurity environment has undergone significant changes, posing intricate obstacles that surpass conventional defensive tactics. The evolution of cyber threats throughout history has illustrated the dynamic and persistent nature of cybersecurity challenges, emphasising the need for a comprehensive security approach.

As mentioned earlier, the shift can be attributed to the swift progress of technology, the heightened complexity of cyber hazards, and the broadening of the areas vulnerable to attack due to the widespread integration of digital tools and methodologies. The increasing overlap between personal and professional utilisation of technology has expanded the possible avenues for cyberattacks. To tackle these obstacles, organisations must allocate resources towards a comprehensive security approach incorporating various layers. This approach should involve technical measures such as firewalls, intrusion detection systems, encryption, and human-centric components such as continuous employee training and security awareness initiatives. In addition, cultivating a security-oriented culture and deploying comprehensive governance frameworks can enhance an

entity's capacity to withstand cyber hazards. The cybersecurity domain's dynamic and constantly changing nature necessitates an ongoing reevaluation of security protocols and a dedication to remaining up-to-date with emerging patterns and optimal methodologies. Within this context, cyber resiliency has surfaced as a crucial facet of an organisation's cybersecurity stance, allowing them to more effectively anticipate, endure, recuperate from, and adjust to unfavourable occurrences amidst the constantly changing landscape of threats. The transition towards a more resilient stance requires a comprehensive strategy that includes technological and organisational measures. Developing comprehensive risk assessment and management processes is a crucial component of a cyber-resilient system. This enables organisations to identify potential vulnerabilities effectively, prioritise mitigation efforts, and allocate resources in a manner that optimises their effectiveness. Moreover, implementing incident response strategies and business continuity procedures guarantees that enterprises can mitigate interruptions and promptly recuperate from any cyber occurrences that might transpire. Collaborating and sharing information among industry peers and establishing public-private partnerships can serve as a means of collective defence and enable organisations to remain apprised of emerging threats and optimal practices. By integrating these principles into their cybersecurity strategies, entities can improve their capacity to adjust and flourish in an ever more intricate and dynamic digital milieu.

Organisations are confronted with elevated risks with the increasing reliance on digital infrastructure. Effective cyberattacks can result in significant ramifications, such as monetary deficits, operational interruptions, harm to reputation, and possible legal accountabilities. Therefore, cyber resiliency holds considerable importance in guaranteeing the uninterrupted functioning of operations, mitigating adverse consequences, and upholding the confidence of clients and interested parties.

The increasing complexity and potential impact of cyberattacks can be attributed to the rising sophistication of cyber threats. These threats include early computer viruses, worms, ransomware, advanced persistent threats (APTs), and state-sponsored cyber warfare. Cyber resiliency enables organisations to enhance their ability to safeguard their

crucial assets and systems against highly advanced threats. This approach ensures prompt recuperation and adjustment during a successful security breach.

The swift advancements in technology, encompassing the advent of innovative technologies such as cloud computing, artificial intelligence, and the Internet of Things (IoT), offer organisations unparalleled prospects for expansion and ingenuity. Nevertheless, introducing these technological advancements presents novel vulnerabilities and attack vectors that adversaries can exploit. The development of cyber resilience enables organisations to effectively mitigate the risks that arise from adopting novel technologies and proactively anticipate potential threats.

In addition, the increasing recognition of cyber threats has led governmental bodies and regulatory agencies within various industries to implement more rigorous cybersecurity protocols to safeguard crucial infrastructure, confidential information, and consumers' privacy. To adhere to regulatory requirements, evade sanctions, and uphold a favourable standing in the industry, entities must exhibit cyber resiliency.

The contemporary phenomenon of globalisation and interconnectivity significantly impacts the swift propagation of cyber threats beyond geographical boundaries, thereby affecting organisations operating in diverse sectors and regions. Organisations can promote the stability and security of the global digital ecosystem and create a safer environment for all stakeholders by improving their cyber resilience.

In light of the constantly changing and intricate threat landscape, organisations must allocate resources towards enhancing their cyber resilience. This is necessary to safeguard crucial assets, guarantee uninterrupted business operations, and sustain their competitive advantage. Adopting a proactive approach will improve their readiness to tackle the obstacles presented by the constantly evolving cybersecurity environment and aid in fortifying the security and stability of the digital ecosystem.

Cyber resilience has emerged as a crucial element in contemporary cybersecurity tactics, catering to the need for businesses to exhibit adaptability and foresight when confronted

with evolving cyber hazards. Cyber resilience pertains to an organisation's ability to withstand, recuperate from, and adjust to cyber-attacks while mitigating their potential consequences on business activities, image, and information authenticity. The conventional approach to cybersecurity concentrates on identifying and preventing cyber threats (Mazzolin and Madni 2020). However, cyber resiliency acknowledges the inevitability of successful attacks and underscores the significance of a holistic strategy encompassing incident response, recovery, and adaptation.

While cyber resiliency and cybersecurity are interconnected, they have distinct objectives (Möller, 2023). Cybersecurity mainly focuses on preventing unauthorised access, disclosure, modification, or destruction of information systems and data through technological, procedural, and human protective measures. The defensive tactic aims to mitigate susceptibilities, detect unauthorised access, and forestall the manipulation of weaknesses in an entity's digital framework.

The concept of cyber resilience acknowledges the inherent limitations of security measures and the inevitability of accidents, despite wide preventive measures. Cyber resilience is the term used to describe an organisation's ability to maintain critical services in the face of a cyber attack, as well as to recover from the incident and adjust to changing threat landscapes. As mentioned earlier, the approach underscores the importance of preparedness, flexibility, and ongoing growth in mitigating the impact of cyber assaults.

Organisations cannot rely solely on preventive measures due to the swift pace of technological advancements and the increasing intricacy of cyber threats. Consequently, organisations must adopt flexible and anticipatory strategies that precede cyber resilience. This approach enables them to promptly identify, address, and recuperate from security breaches while consistently enhancing their protective measures to avoid potential risks.

The defence-in-depth approach involves implementing multiple security measures throughout an entity's information technology infrastructure, including its data, networks, and systems. The concept of defence-in-depth aims to mitigate the risk of a successful intrusion by implementing multiple layers of security controls so that in the event of a

failure of one power, others will remain effective in defending the system. The approach integrates preventive, detective, and corrective measures such as firewalls, intrusion detection systems, encryption, and incident response teams.

Threat intelligence is the systematic process of collecting, examining, and distributing data on current and potential cybersecurity threats. By constructing a comprehensive understanding of the threat landscape, organisations can enhance their ability to anticipate future attacks, pinpoint vulnerabilities, and allocate resources to cybersecurity activities more effectively. Threat intelligence can be derived from various sources, including open-source intelligence, industry-specific threat feeds, and commercial threat intelligence providers.

Developing and regularly maintaining an incident response plan is imperative for organisations to handle and remediate cyber incidents proficiently. The goal should delineate roles and responsibilities, communication modalities, and procedures for detecting, mitigating, eradicating, and remediating an incident. Systematic training, exercises, and simulations can enhance an organisation's preparedness to respond effectively to an incident while also identifying potential areas of improvement in the response protocol.

Continuous monitoring and assessment of an organisation's networks, systems, and data facilitate the timely identification of potential risks and vulnerabilities (Malatji, Marnewick, and Solms 2022). Periodic evaluations, such as vulnerability scans, penetration testing, and security audits, can facilitate the detection of weaknesses and vulnerabilities in an entity's cybersecurity stance, thereby allowing for timely remediation and enhancements.

Implementing business continuity and disaster recovery strategies is crucial for organisations to ensure the continuity of their critical operations during a cyber incident (Möller 2023). While business continuity planning aims to sustain the organisation's essential functions during and after such an event (Margherita and Heikkilä 2021), disaster recovery focuses on restoring systems, applications, and data following a

disruption (Danquah, Bekoe, and Gordon 2022). Establishing and regularly revising business continuity and disaster recovery plans, encompassing the recognition of critical systems and procedures, recovery objectives, and strategies for restoring standard operations, constitute a crucial component of cyber resilience.

Cyber risk management is the systematic approach of identifying, assessing, and mitigating risks associated with an organisation's information systems and networks. The process, as mentioned above, involves;

- evaluating the probability and magnitude of potential hazards,
- implementing good security protocols to mitigate risk to a tolerable degree, and
- overseeing the effectiveness of said measures.

Incorporating cyber risk management into the broader enterprise risk management framework of an organisation can aid in ensuring that cyber threats are effectively managed and prioritised.

Establishing an organisational culture that prioritises security knowledge and accountability among employees is a critical factor in the effectiveness of a cyber resilience initiative. Regular training and awareness initiatives are advantageous for employees as they aid in comprehending their responsibility in safeguarding the organisation's information assets and recognising common attack vectors, such as phishing and social engineering (Bauer, Bernroider, and Chudzikowski 2017). In addition, leaders' strong commitment and resilience to cybersecurity facilitate the adoption of best practices and ensures adequate resources are allocated for these efforts.

The growing dependence on information technology and interconnected networks in the digital era has shifted from conventional cybersecurity approaches to a more holistic and proactive emphasis on cyber resilience. Implementing crucial principles and strategies, such as defence-in-depth, threat intelligence, incident response planning, continuous monitoring, and fostering a security-aware culture, can enhance an organisation's resilience against the dynamic and persistent challenges of cyber threats. Investing in

cyber resilience has the potential to mitigate the impact of cyber catastrophes on corporate operations and reputation. Additionally, it can aid enterprises in sustaining a competitive edge in a progressively digitised and interconnected world.

Regulatory frameworks and information security standards are crucial in shaping and directing cybersecurity and cyber resilience (Lykou, Anagnostopoulou, and Gritzalis 2018). The frameworks and standards outlined offer a comprehensive collection of optimal methodologies, guidelines, and mandates for organisations to utilise when constructing, executing, and upholding professional cybersecurity and cyber resiliency initiatives (Chopra and Chaudhary 2020).

Several regulatory frameworks and information security standards have emerged to tackle different aspects of cybersecurity and cyber resilience. Several examples of widely recognised frameworks and standards in information security include ISO/IEC 27001, the NIST Cybersecurity Framework, GDPR, ITIL, COBIT, and CIS Critical Security Controls. By adhering to established frameworks and standards, organisations can enhance their security stance, mitigate the likelihood of cyber incidents, and exhibit dedication to safeguarding sensitive data and systems.

Adherence to regulatory frameworks and standards can yield significant financial benefits for organisations (Sharma and Dash 2012). Initially, their role involves aiding organisations in devising a deliberate and methodical approach to managing cybersecurity threats, guaranteeing comprehensive coverage of all aspects of their security stance (Sharma and Dash 2012; Chopra and Chaudhary 2020). Adopting a comprehensive strategy could lead to enhanced security measures, reducing the probability of security breaches and incidents and improving operational efficiency (Lykou, Anagnostopoulou, and Gritzalis 2018).

Adherence to established frameworks and standards can serve as a means for businesses to showcase their dedication to ensuring security and privacy. This could foster trust among customers, stakeholders, and regulatory bodies. In a world that is becoming more

interconnected, establishing trust is paramount in maintaining a favourable reputation and ensuring sustained business prosperity.

Regulatory frameworks and standards often function as benchmarks for industry best practices, aiding organisations in remaining current on the latest security threats, vulnerabilities, and mitigation strategies. Acquiring this knowledge may assist enterprises in adjusting and enhancing their cybersecurity and cyber resiliency endeavours in reaction to a dynamic threat environment, guaranteeing their preparedness for novel and developing threats.

Regulatory frameworks and information security standards are significant factors that influence organisations' cybersecurity and cyber resilience endeavours. By implementing and following these guidelines and standards, organisations can enhance their security stance, exhibit their dedication to safeguarding sensitive information and systems, and enhance their readiness to counter the constantly evolving cyber threats of the digital era. Organisations encounter various obstacles in attaining cyber resilience, despite the growing significance of this concept and the support offered by regulatory frameworks and standards. The challenges above stem from limited resources, inadequate personnel training, and rapidly evolving threat landscapes. This section comprehensively analyses the issues mentioned earlier and presents case studies of companies that have encountered challenges in building cyber resilience. Moreover, it highlights the intricacies of quantifying an entity's resilience, compounding these challenges.

The challenge of resource scarcity is a significant impediment businesses encounter when striving to enhance their cyber resilience. Establishing and sustaining a robust cybersecurity and cyber resilience scheme requires substantial technology, infrastructure, and personnel resources. The budgetary limitations may challenge numerous companies, especially small and medium-sized enterprises (SMEs), in justifying or executing these investments. Resource limitations may prompt organisations to compromise their cybersecurity and cyber resilience measures, exposing them to cyber attacks.

Ransomware attacks are more common for large enterprises than for SMEs, but SMEs were disproportionately hit by them in 2018 (Connolly et al. n.d.); according to the study of Connolly et al., n.d., pertains to the considerable number of small and medium-sized enterprises (SMEs) subjected to ransomware assaults in the past few years. The insufficiency of cybersecurity and cyber resilience resources allocated to these companies often results in inadequate protection and response mechanisms, rendering them vulnerable to cybercriminal attacks. The gravity of the impact of ransomware attacks on these companies underscores the importance of prioritising investments in cyber resilience and highlights the challenges organisations with limited resources encounter.

A lack of skilled personnel represents an additional obstacle to establishing cyber resilience (S. Furnell 2021). The rapid progression of information technology, coupled with the escalating complexity of cyber threats, has led to a surge in the need for proficient cybersecurity professionals (Mailloux and Grimailla 2018). Regrettably, supply insufficiency has failed to match the demand, culminating in a critical dearth of competent cybersecurity personnel (Turnbull 2018). The limited availability of qualified personnel has posed a difficulty for organisations to attract and retain the workforce necessary to develop and maintain robust cybersecurity and cyber resiliency initiatives (Turnbull 2018).

The dynamic and evolving nature of the threat landscape presents a significant obstacle to achieving cyber resilience. The landscape of cyber threats is constantly changing, with novel avenues and tactics for attacks emerging with frequency. Organisations must stay abreast of technological advancements and adapt their cybersecurity and cyber resilience policies accordingly. Nevertheless, even for organisations with ample resources, the pace of transformation and the sheer quantity of emerging hazards can be intimidating.

Even with a comprehensive cybersecurity program and a committed team of experts, the enterprise may be unsuccessful in thwarting the breach because of the novel *modus operandi* of an attack. The numerous instances exemplify the challenge of maintaining an advantage over the constantly evolving threat environment, underscoring organisations' need for adaptability and foresight to fortify their cybersecurity measures.

The intricacy of assessing an organisation's strength and resilience contributes to the abovementioned challenges. Although several frameworks and metrics exist to evaluate the cybersecurity posture, measuring resilience must be completed and discovered. This is because resilience encompasses the capacity to avert and identify hazards and the capacity to rebound and adjust in the presence of hardship. This research offers a measurable perspective on resilience that considers an organisation's unique needs, its appetite for risk, and the "ability control" indicators that align with worldwide standards. This methodology circumvents strict rules and mandates. Adhering to regulations without acknowledging ability may result in standardisation, but it does not facilitate resilience assessment. Assessing an entity's capacity to rebound from and adjust to adverse circumstances requires a thorough methodology considering various factors, such as corporate culture, physical facilities, procedures, and personnel.

Cyber resiliency has emerged as a distinct phenomenon in response to the dynamic and intricate nature of the contemporary threat landscape, which has been constantly evolving. The conventional approach to cybersecurity is centred on thwarting unauthorised access to networks, information, and systems. Conversely, cyber resiliency guarantees that entities can sustain critical operations and promptly recuperate from cyber assaults or system malfunctions. The change above in focus accentuates the necessity for entities to exhibit adaptability and foresight in confronting developing cyber hazards instead of depending exclusively on defensive tactics.

The acknowledgement that no entity can be entirely impervious to cyber threats has emerged as a crucial impetus behind advancing cyber resiliency. It has become evident that a solely responsive strategy towards cybersecurity needs to be improved, given the emergence of novel tactics by attackers and their exploitation of nascent vulnerabilities (Bodeau, Graubart, and Bedford 2017). Organisations must adopt a comprehensive and proactive approach whereby they anticipate potential threats and devise strategies to mitigate their impact (Bodeau, Graubart, and Bedford 2017).

Defence-in-depth is a crucial aspect of cyber resiliency (Ahmadi-Assalemi et al. n.d.), underscoring the significance of employing several security layers to safeguard an organisation's resources. The defence-in-depth approach advocates for utilising multiple layers of protection across different levels, encompassing physical, technical, and procedural controls, instead of solely depending on a single security measure (Bodeau, Graubart, and Bedford 2017). This methodology guarantees that supplementary layers of security can effectively restrict the breach and mitigate its consequences in the event of a breach in one layer of protection.

By actively monitoring and assessing their internal processes and the threat landscape and gathering information about emerging risks and vulnerabilities, organisations can enhance their ability to anticipate potential attacks and implement appropriate countermeasures. Adopting a proactive approach enables organisations to maintain a competitive edge over potential attackers, thereby decreasing the probability of successful breaches and mitigating the impact of any that may occur.

Developing a response plan for incidents is crucial to ensuring cyber resilience. Organisations must acknowledge that security breaches and system failures are inevitable. Therefore, they must establish comprehensive incident response strategies to promptly detect, confine, and resolve any security incidents that may arise. The development of specific procedures and guidelines is imperative for incident response planning to be effective. Additionally, regular testing and updating of these plans are crucial to maintaining their efficacy in light of emerging threats.

The significance of ongoing enhancements in cyber resiliency cannot be overstated, as it underscores the imperative for entities to consistently evaluate and enhance their cybersecurity and cyber resiliency protocols. Periodic security posture assessments enable organisations to identify deficiencies and vulnerabilities in their security measures, prioritise remedial actions, and implement necessary modifications to mitigate emerging threats. The continuous evaluation and enhancement of one's cyber resilience stance are imperative to uphold a robust defence against the ever-evolving threat environment.

The distinct concept of cyber resiliency, as different from cybersecurity, highlights the need for organisations to adopt a more proactive and adaptable approach to tackling the constantly evolving threat landscape. Implementing fundamental principles and strategies, such as defence-in-depth, threat intelligence, incident response planning, and continuous improvement, can enhance an organisation's capacity to endure and recuperate from cyberattacks and system failures. Organisations must adapt their strategies and measures to maintain cyber resilience in response to the changing cyber threat landscape.

1.2 Objectives and Scope of the Thesis

The primary objective of this research is to develop and implement a comprehensive auditing approach that employs persona-based and risk-based capability control metrics to assess an enterprise's capacity to withstand cyber threats. In the current dynamic landscape of cyber threats, organisations must possess robust cybersecurity protocols and a resilient degree to recover from potential cyber incidents.

This research aims to advance cyber resiliency by devising a novel and productive approach for assessing an entity's capacity to prevent, detect, and remediate cyber hazards.

The approach endeavours to comprehensively assess an entity's capacity to withstand cyber threats by employing a combination of persona-driven and risk-driven ability control metrics. Persona-based metrics consider the diverse roles and responsibilities held by individuals within an organisation and the varied perspectives and potential limitations that may arise from these roles. In contrast, metrics based on risk assessment examine an organisation's approach to identifying, assessing, and mitigating cyber risks, as well as aligning these measures with the organisation's overarching risk management framework.

The study aims to provide organisations with valuable insights into their existing cyber resiliency posture, identify potential areas for enhancement, and facilitate informed decision-making regarding investments in cyber resiliency utilising the proposed audit methodology. The primary objective of this study is to establish a robust correlation

between the cyber resiliency rating of an enterprise and its adherence to diverse information security protocols.

The alignment of organisations with industry best practices and regulatory requirements will provide a distinct pathway for enhancing their cyber resiliency.

The following are the key research issues that are intended to be answered by this thesis:

1. Using persona-based and risk-based ability control metrics, what are some effective ways to measure the cyber resiliency of an organisation?
2. What is the correlation between the cyber resiliency scores of firms and the extent to which they comply with the various information security standards?

To answer the first research question, it is essential to fully understand the main ideas driving persona-based and risk-based ability control metrics. This understanding must also include an examination of the benefits and drawbacks associated with each of these metric types. Metrics that are persona-based for ability control emphasise employees' many roles and tasks within a company. These metrics also consider the distinct points of view and potential risks associated with these positions. By taking into account the human element of cybersecurity, this research has shown that; persona-based metrics can assist businesses in recognising and addressing any vulnerabilities in their security posture caused by their personnel's actions and behaviours.

Conversely, risk-based ability control metrics focus on an organisation's strategy for recognising, assessing, and mitigating cyber threats. They emphasise aligning these activities with the overall risk management strategy of the business. By utilising metrics based on risk, companies can ensure that their actions to improve their cyber resilience are driven by a full understanding of the potential dangers they face and the most effective methods for mitigating those risks.

The following are some of the measures that can be performed to properly monitor cyber resiliency with persona-based and risk-based ability control metrics:

- a. Acquire a comprehensive knowledge of the structure of the organisation, as well as the roles and responsibilities within it.
- b. Recognise and create a map of the organisation's most significant potential cyber risks and vulnerabilities.
- c. Conceive and put into practice an all-encompassing audit methodology that considers persona-based and risk-based ability control metrics.
- d. Based on the audit results, evaluate the organisation's cyber resiliency posture, indicating areas in which improvements can be made and best practices that should be applied.
- e. Monitor and keep track of the organisation's progress in addressing the identified vulnerabilities and improving its overall cyber resiliency.

The second research question aims to understand better the connection between enterprises' cyber resiliency ratings and the information security standards those organisations adhere to. To find an answer to this question, it is necessary to investigate the association between the cyber resiliency ratings attained due to the audit methodology and the businesses' level of compliance with the applicable information security standards. The following are some possible ways to carry out this analysis:

1. Recognising the primary information security standards pertinent to the organisations being audited, including but not limited to ISO/IEC 27001, NIST, GDPR, ITIL, COBIT, and CIS, amongst others.
2. Determining the extent to which the organisations conform to these standards, considering the organisations' policies, processes, and controls and the documentation of those aspects.
3. Determining whether or not there is a significant association between the firms' cyber resiliency scores and compliance levels by comparing the two and seeing whether there is a relationship between the two.

The results of this analysis, which will be provided as a byproduct of the research, are expected to yield important insights into the degree to which adherence to information security standards contributes to the overall cyber resiliency of a business. This will allow organisations to prioritise their investments in cyber resilience projects more effectively, concentrating on areas of their security posture most closely aligned with industry best practices and regulatory requirements. This will allow organisations to prioritise their investments in cyber resilience programs more effectively.

In conclusion, addressing these research topics will contribute to the continued development of efficient cyber resiliency assessment methodologies and expand our understanding of the relationship between cyber resiliency and compliance with information security standards. Cyber resiliency refers to the degree to which an organisation can withstand cyberattack threats. This research will ultimately help boost the security and resilience of our increasingly interconnected digital ecosystem by giving companies the tools and insights necessary to measure and improve their cyber resiliency posture. This will be accomplished by providing organisations with the tools and insights to measure and improve their cyber resiliency posture.

This study aims to develop and implement an audit approach that employs persona and risk-based capability control metrics to assess the cyber resiliency stance of an entity. This study will centre on organisations of varying sizes, including small-to-medium, medium, and large enterprises, as well as a university. This study aims to provide a comprehensive understanding of the determinants of cyber resiliency in varying circumstances by examining organisations with diverse structures, resources, and levels of operational complexity.

The present investigation will employ evaluation kits encompassing a broad spectrum of information security norms, including but not limited to ISO/IEC 27001, NIST, GDPR, ITIL, COBIT, and CIS. The present study aims to ensure that the audit methodology adheres to industry best practices and caters to diverse security requirements by utilising these standards in developing assessment kits.

Despite the comprehensive nature of this study, certain factors must be considered. To adhere to ethical principles, the confidentiality and anonymity of all participating organisations in this study will be upheld to safeguard their privacy. Implementing security measures ensures the preservation of confidential data, albeit potentially impeding the contextualisation and comparative analysis of outcomes concerning specific industrial or organisational profiles.

The study has obtained consent forms and consent from all participating organisations regarding their support and participation. The possibility of a self-selection bias arises as a consequence of the fact that only those organisations that express interest in participating will be included in the study. This may pose a challenge in generalising the findings to a broader population.

The evaluation kits encompass a broad spectrum of information security standards; however, it is only feasible to incorporate some measures that may hold significance to the audited groups. Consequently, certain facets of an organisation's security may have yet to undergo comprehensive assessment or discourse within the purview of this investigation.

The constant emergence of novel attack vectors, techniques, and vulnerabilities characterises the dynamic nature of the cyberspace threat landscape. The present investigation is grounded in existing knowledge about cybersecurity. Due to this, the study's outcomes may require periodic revisions and modifications in response to emerging risks and optimal methodologies.

The assessment process may contain subjectivity despite utilising the audit method developed in this study, which is grounded in established information security standards. This phenomenon may be attributed to divergent perspectives among organisations regarding the interpretation of standards or to varying obstacles and hazards encountered by different organisations. It is imperative to consider the potential biases and limitations when interpreting the findings of this study.

The primary objective of this research is to provide valuable insights into the cyber resilience of organisations of varying sizes and types. This is achieved by implementing a comprehensive audit methodology that adheres to established information security standards. Disclosing the study's limitations facilitates comprehension and utilisation of the findings by providing insight into the factors that could impact their credibility and generalizability.

1.3 Overview of the Methodology

A pivotal aspect of this research entails the development of two evaluation kits that centre on ability control metrics based on risk and persona. The production of these kits is a highly intricate process that can be briefly outlined in the subsequent stages:

The initial stage in the development of assessment kits involved the selection of appropriate control metrics. As mentioned, the appointments were made after a comprehensive evaluation of globally recognised benchmarks of information security and information technology management domains. The measure, as discussed above, ensured that the control measures implemented in the assessment kits were consistent with the most effective techniques employed in the industry and encompassed a diverse spectrum of security requirements.

The cyber resiliency problem can be defined as the need for a quantifiable means of assessing an organisation's ability to withstand and recover from cyber-attacks. To address this issue, developing a scoring system that assigns numerical values to an organisation's level of resiliency has been deemed necessary. Every testing kit was designed to provide a numerical score up to a maximum of 100. The composite cyber resiliency score of the organisation was determined by aggregating the outcomes of both evaluation kits and assigning a specific weight to each.

The primary characteristic of the risk-based assessment kit was its comprehensive risk evaluation procedure before conducting the audit. The abovementioned process facilitated the identification of the organisation's most significant hazards and vulnerabilities, which were subsequently remedied through the implementation of control

metrics employed during the review. The risk-based kit provided a comprehensive and focused cyber resilience assessment by tailoring the survey to align with the specific risk profile of each organisation.

The persona-based assessment kit aimed to identify the organisation's primary personas and assign each individual a "zero-trust" rating. This approach considered the significance of personnel in maintaining cyber resilience and endeavoured to evaluate the efficacy of a company's zero-trust framework in managing insider threats and access control.

After completing the assessments, an audit report was generated and disseminated to the participating groups. As mentioned, the words evaluated the organisation's cyber security rating and identified any non-compliance or vulnerabilities. The reports provided a list of relevant global information security standards and associated articles deemed significant to address the identified organisational gaps.

The risk-based and persona-based assessment kits were developed through a rigorous process involving a comprehensive examination of information security standards, establishing a clearly defined scoring mechanism, and various approaches to appraise an entity's cyber resiliency per its risk profile and personnel composition. The study aims to assist various organisations in developing robust and dependable cybersecurity strategies by providing them with comprehensive audit reports highlighting improvement areas and offering recommendations on optimal practices.

The significance of this research lies in its potential to assist organisations in comprehending and enhancing their capacity to withstand and recover from cyber threats. The present investigation endeavours to tackle the inadequacies of current frameworks and metrics to gauge an organisation's resilience. This is achieved by introducing a novel approach to measuring cyber resiliency that involves the utilisation of persona- and risk-based ability control metrics. This approach aims to provide a more accurate and comprehensive depiction of an entity's capacity to mitigate, detect, and remediate cyber hazards.

A salient aspect of this study pertains to examining the distinct requirements of individual organisations, encompassing factors such as their risk appetite, organisational ethos, infrastructure, protocols, and personnel. The present investigation circumvents the utilisation of a uniform approach that may result in homogenisation without adequately assessing the level of resilience exhibited by an organisation. Rather than employing a standardised process, it utilises a tailored methodology that conforms to established international norms for information security.

Organisations must have precise standards and corresponding articles integral to their audit reports. This constitutes a significant component of the present investigation. The current study highlights potential vulnerabilities by identifying the shortcomings and domains where enterprises may be deficient in their endeavours towards cyber resiliency. Moreover, it provides practical guidance to organisations on how to address these gaps. Implementing this focused approach equips organisations with the necessary insights to make informed decisions regarding their cybersecurity strategies, enhancing their ability to counteract constantly evolving cyber threats.

Moreover, developing two assessment packages centred on risk-based and persona-based metrics for capability management can generate novel concepts in cyber resilience. This study expands the boundaries of our understanding of resilience by presenting a novel perspective that considers an organisation's distinct risk profile and personnel composition. Furthermore, it promotes further investigation into the development of precise and comprehensive evaluation techniques.

The significance of this study lies in its potential to contribute to advancing the field of cyber resiliency by providing a comprehensive and novel approach to assessing an organisation's capacity to prevent, detect, and respond to cyber hazards. This study has the potential to significantly impact the development and implementation of effective cybersecurity strategies across various organisations by providing them with precise and practical recommendations based on global information security standards.

2. LITERATURE REVIEW

2.1 Brief History of the Internet

The Internet is a worldwide network of interconnected computer systems that employ standardised communication protocols to exchange information and services. The Internet is a complex system comprising interconnected networks encompassing public and private entities, including academic institutions, organisations, businesses, and government agencies. These networks are connected through various wired, wireless, and satellite technologies.

The Internet holds immense significance in the contemporary digital era. The advent of technology has brought about a significant transformation in various facets of contemporary society, including communication, commerce, education, entertainment, and other domains (Kaushik and Bagga 2020). The technology allows for immediate data retrieval, eliminates limitations imposed by physical location, and fosters cooperative efforts among individuals separated by distance. The advent of the Internet has catalysed innovation, facilitated novel business prospects, and reconfigured social dynamics.

The origins of the Internet can be traced to the late 1960s and early 1970s when the Advanced Research Projects Agency (ARPA) of the United States Department of Defense developed the ARPANET. This pioneering network served as a foundation for the contemporary Internet. The primary goal of the ARPANET was to establish a communication system that could sustain its functionality in the event of a nuclear attack, thereby facilitating the exchange of information among military installations and researchers (Ryan 2010).

The inception of the Internet can be attributed to the late 1960s and early 1970s, during which the Advanced Research Projects Agency (ARPA) of the United States Department of Defense established the ARPANET. This pioneering network established the foundation for the contemporary Internet. The primary objective of the ARPANET was to establish a robust communication infrastructure that could sustain its operations even

in the event of a nuclear attack, thereby facilitating the exchange of information among military bases and scholars.

A brief history of ARPANET is a network of computers that can talk to each other. It was built by the Advanced Research Project Agency (ARPA), which later changed its name to the Defense Advanced Research Project Agency (DARPA) (Packard 2020).

During the 1950s, a period of political tension known as the Cold War was ongoing, and subsequently, the development of the Internet commenced (Targowski 2005). The significance of nuclear weapons was crucial to the war (Ryan 2010). Utilising nuclear weapons has also disrupted the integrity of command-and-control systems of security. In this particular scenario, exercising caution while handling said armaments was deemed crucial. According to Ryan (2010), the side with the most dependable command and control system was victorious during the Cold War.

The concern pertains to the potential disruption of FM radio transmission in the stratosphere due to a plausible nuclear explosion. This scenario is analogous to the hypothetical scenario of a nuclear attack on the earth's surface, which could collapse the national phone network operated by the American Telephone and Telegraph Company (AT&T). As a result of these findings, both parties were compelled to consider the concept of mutually assured destruction (MAD). As mentioned earlier, the rationale remains valid: retribution would be unfeasible if the assault caused impairment to the communication infrastructure of either party.

According to RAND, enhancing communication networks would be the most effective approach for the parties involved in the Cold War to address this issue (Targowski 2005). The solution devised by RAND was groundbreaking in several respects, as it established the foundation for the Internet (Ryan, 2010).

Subsequently, ARPA underwent a name modification to ARPANET, enabling interconnected computers within the network to transmit and receive small data packets.

The transmission of the word "lo" from a computer located at the University of California (UCLA) to another computer situated at the Stanford Research Institute (RSI), separated by a distance of approximately 600 kilometres, occurred on October 29, 1969 (Packard 2020). This marked the initial instance of a successful establishment and termination of a computer connection. After this event, the network experienced rapid expansion, and as of 1971, it comprised 14 nodes. Since 1973, numerous connections to ARPANET have been established. Consequently, the development of standardised communication protocols facilitated interoperability among networks. Since the latter part of the 1970s, individuals have employed technological methodologies such as Transmission Control Protocol (TCP) and Internet Protocol (IP) (Ryan 2010).

By utilising these protocols, it has been determined how information is segmented into discrete units for transmission, thereby enabling intercommunication among networked computing devices. The Internet Protocol (IP) determines data transmission between IP addresses. In contrast, Transmission Control Protocol (TCP) ensures the sequential delivery of data packets, which is not a User Datagram Protocol (UDP) feature. This is the origin of the Internet.

During the 1980s, the development of the Internet was advanced through the implementation of the Transmission Control Protocol (TCP) and the Internet Protocol (IP), which collectively established the fundamental framework of the TCP/IP protocol suite. This advancement facilitated the interconnection of numerous networks, laying the foundation for the contemporary Internet.

The emergence of the World Wide Web in 1989, credited to Tim Berners-Lee, a renowned British computer scientist, signified a pivotal juncture in the progression of the Internet (Berners-Lee 2010). The World Wide Web furnished a user-friendly platform for retrieving and disseminating data on the Internet via hyperlinks and web browsers. In 1993, the initial web browser, Mosaic, was unveiled, enabling a wider audience to access the Web and propelling its swift proliferation (Vetter, Spell, and Ward 1994).

During the timeframe spanning from the 1970s to the 1990s, the Internet experienced a significant surge in usage, diverging from its original purpose as a backup communication channel (Kergel 2019). This shift in usage contributed to the Internet's widespread popularity during this era. Internet utilisation was subject to differentiation based on ideological perspectives during these periods. For instance, it served as a valuable means for exchanging information without cost. Moreover, the Internet inherently possesses an independent and diversified architecture. This results in diverse cultural pursuits and a tabula rasa upon which to envision concepts for improved, more liberated societies.

Furthermore, it is widely acknowledged that the Internet has provided a platform for individuals to interact socially (Kergel 2019). In addition to the advantages offered by the Internet, it has also provided a platform for activism. The "Hacker Manifesto," authored by Mentor in 1986, is a notable early instance of this phenomenon (S. M. Furnell, Dowland, and Sanders 1999).

The infrastructure and accessibility of the Internet have undergone significant evolution over time. The advent of broadband connectivity during the late 1990s and early 2000s facilitated expedited data transfer rates, augmenting the end-user experience and propelling the expansion of data-intensive applications such as online gaming and video streaming (Curran, Fenton, and Freedman 2012).

The advent of mobile devices, specifically smartphones and tablets, during the latter part of the 2000s and early 2010s, brought about a transformation in the manner in which individuals obtained access to the Internet; in the year 2016, the usage of mobile Internet surpassed that of desktop internet (Singh and Swait 2017), thereby emphasising the growing significance of mobile connectivity in the contemporary digital era.

The development of the Internet has been influenced by the advent of novel technologies and services, including but not limited to cloud computing, the Internet of Things (IoT), and social media platforms (Kaushik and Bagga 2020). The advent of cloud computing has significantly transformed how data and services are stored and retrieved, offering flexible and readily available computing resources. The Internet of Things (IoT) has extended the scope of the Internet to encompass commonplace objects, thereby

facilitating the exchange of information among devices without requiring human intervention. Social media platforms have significantly transformed communication and information dissemination, facilitating the instantaneous sharing of news, concepts, and viewpoints.

The Internet is an extensive and interconnected network that has fundamentally transformed our way of life, employment, and communication in the digital era. The origins of its development can be traced to the ARPANET during the late 1960s. Subsequently, it has undergone significant evolution through the introduction of the World Wide Web, the proliferation of broadband and mobile connectivity, and the emergence of novel technologies and services. The ubiquitous influence of the Internet is apparent in its far-reaching effects on diverse facets of contemporary society, encompassing domains such as interpersonal interaction, economic transactions, scholastic pursuits, and recreational activities.

2.2 Brief History of Cybersecurity

Cybersecurity encompasses the implementation of methodologies, procedures, and technological solutions to safeguard digital data, computer systems, and networks from unauthorised access, utilisation, dissemination, interference, or obliteration by unauthorised individuals. The field of study under consideration holds significant relevance for individuals, corporations, and governing bodies that rely on digital infrastructure for various purposes, such as communication, data retention, monetary dealings, and essential amenities.

The advent of the digital era has ushered in an era where interconnected systems and ubiquitous computing have become the norm. The significance of cybersecurity has elevated to a main level for individuals and enterprises globally. A corresponding rise in the likelihood of cyber threats accompanies the increasing dependence of individuals on digital technologies. These threats in financial losses harm a company's reputation, disruption, and even jeopardise national security. It is imperative to implement cybersecurity protocols to safeguard confidential data, ensure the integrity and availability of digital infrastructures, and foster confidence in the digital realm.

The field has been the imperative field of cybersecurity since the inception of computer systems, with an initial emphasis on safeguarding mainframe computers and ensuring the confidentiality of data. With the evolution and proliferation of networking technologies, particularly with the advent of the Internet, the emphasis has shifted towards ensuring the security of networked systems and preventing unauthorised access.

The proliferation of viruses and worms during the 1980s necessitated the development of antivirus software and other security measures to counteract these emerging threats. During this period, there was a concurrent emergence of the hacker community (Holt, 2020), comprised of proficient individuals who sought to exploit vulnerabilities in computer systems vulnerabilities for various cities and experiment with malicious intent.

During the 1990s, there was a rapid expansion of the Internet rapid expansion-commerce (Ankush, 2020). Consequently, robust security protocols were necessitated to safeguard online transactions and sensitive personal data. The objective of encryption technologies such as Secure Encryptionnsport Layer Security (TLS) is to facilitate the secure transmission of confidential information over networks, thereby preventing unauthorised interception. Moreover, enterprises have begun implementing routers and intrusion detection systems to monitor and regulate network traffic. This measure monitors and regulates access or data theft.

The advent of Advanced Persistent Threats (APTs) exacerbated cyber threats in the early 2000s (Y.-K. Kim et al., 2020). Also, numerous standards, frameworks, and benchmarks developed during this period, including but not limited to the NIST Cybersecurity Framework, ISO/IEC 27001, and CIS Critical Security Controls. Subsequently, numerous entities seeking to enhance security have adopted the tactics above, frameworks, and benchmarks.

During the latter part of the 2000s and the initial years of the 2010s, there was a surge in the adoption of cloud computing (Surbiryala & Rong, 2019). Transitioning from on-premises technology to cloud-based services necessitated a distinct approach to managing data and program security. Organisations were required to modify their security strategies

to accommodate the distinct vulnerabilities and susceptibilities of cloud platforms, including but not limited to data breaches, insider hazards, and supply chain assaults (Surbiryala & Rong, 2019).

Simultaneously, the proliferation of mobile gadgets such as smartphones and tablets has amplified the significance of safeguarding these endpoints (Almaiah et al., 2021) since cyber attackers have started to focus on them to exploit vulnerabilities in mobile operating systems and applications. The ubiquitous adoption of mobile devices has resulted in the consumerisation of IT, thereby rendering it increasingly challenging to distinguish between personal and professional digital environments, consequently exacerbating the intricacies of cybersecurity.

The concept of "cyber resiliency" has gained significant prominence in defence over recent years. Resilience is an organisation's capacity to maintain optimal and secure operations despite online hazards or incidents. This approach acknowledges the inevitability of cyber-attacks and emphasises preparedness, rapid response, and efficient recovery for organisations.

The advent of advanced technologies such as artificial intelligence (AI) and machine learning has presented novel opportunities and challenges for cybersecurity (Kaloudi & Jingyue, 2020). From one perspective, these technologies possess the potential to enhance the detection and response to hazardous situations (Abdullahi et al., 2022), thereby facilitating businesses in identifying and mitigating online risks. Conversely, proficiently skilled adversaries can leverage artificial intelligence and machine learning techniques to enhance the intricacy of their cyber offensive operations (Kaloudi & Jingyue, 2020). Consequently, the exigency for sophisticated security protocols is imperative in thwarting these dynamic and evolving hazards.

Organisations are adopting a multi-layered cybersecurity strategy known as defence-in-depth in response to the dynamic nature of online threats. This methodology employs a multi-faceted approach to safeguard digital resources and infrastructures from various angles by implementing multiple layers of security controls. This reduces the probability

of a successful cyber attack. The approach utilised in this method is grounded on fundamental principles and optimal methodologies such as "least privilege," "secure by design," and "continuous monitoring and improvement."

To summarise, cybersecurity holds significant significance in the contemporary era of technology as it safeguards digital information, systems, and networks against unauthorised access or disruption by malicious actors. The evolution of cybersecurity has been closely intertwined with the advancements in digital technologies. The security measures initially implemented for mainframes have undergone significant transformations, and contemporary organisations now rely on multi-layered defences to safeguard themselves against the diverse array of cyber threats that exist today. The evolution of the digital realm is expected to bring forth novel challenges and prospects for cybersecurity experts. In order to safeguard the integrity and accessibility of digital resources and services, cybersecurity experts must remain vigilant and adaptable in the face of emerging risks.

2.3 Cybersecurity Concepts, Definitions, And Related Terminology

Resilience is defined in various exclusive dictionaries as the capacity of an entity to recover swiftly from difficulties or adversity and adapt to changing conditions. This concept forms the premise of cyber resiliency when applied to cybersecurity. Cyber resiliency refers to an organisation's capacity to maintain its digital assets and systems' availability, confidentiality, and integrity despite cyber threats or incidents.

The relationship between the dictionary definition of resilience and cyber resiliency is intricately intertwined. Both concepts highlight the significance of adaptability, recovery, and perseverance in facing obstacles. Cyber resiliency refers to implementing proactive and reactive measures and responses that enable an organisation to anticipate, withstand, and quickly recover from cyberattacks and other security vulnerabilities.

Cybersecurity is the discipline of protecting digital data, systems, and networks from unauthorised access, theft, or damage. It encompasses a vast array of policies, procedures, and technologies designed to protect the confidentiality, integrity, and accessibility of

digital assets. The significance of cybersecurity in the digital age cannot be undeniable, as the increasing reliance on digital technologies exposes organisations and individuals to many cyber threats that can have serious consequences for privacy, commerce, and national security.

In conclusion, the general understanding of resilience serves as a foundation for developing cyber resiliency, which concentrates on protecting and recovering digital assets in the face of cyber threats (Ross et al., 2021b). Cyber resiliency adds a layer of preparedness by emphasising adaptability and rapid recovery from adverse events (Ross et al., 2021b). While cybersecurity is a broader discipline geared at defending against unauthorised access and disruptions, cyber resiliency adds a layer of preparedness by emphasising adaptability and rapid recovery. Incorporating resilience into cybersecurity strategies is crucial for organisations to thrive in the digital era, where the dynamic nature of cyber threats necessitates a proactive and adaptable approach to protecting vital assets and systems.

It is critical to differentiate between security and resilience within cybersecurity to comprehend the distinct methodologies employed to protect digital resources. In information technology, security is the set of measures and technologies to safeguard an organisation's digital infrastructure and data from unauthorised access, use, or harm. Resiliency refers to an organisation's capacity to endure and recuperate from security incidents and disruptions, thereby guaranteeing the uninterrupted functioning of its operations and services.

Taxonomy is a classification and organisational system that has its origins in the field of biology. It involves grouping complex information based on shared characteristics. Establishing a taxonomy for cyber resiliency within the resilience framework facilitates a systematic comprehension of the diverse constituents, including strategies, capabilities, and metrics, that are indispensable for an entity to adeptly adjust and counteract cyber hazards. The implementation of this taxonomy has the potential to enhance the formulation of all-encompassing and consistent strategies aimed at enhancing cyber resiliency in diverse organisations and industries.

From another point of view, a framework refers to a systematic collection of principles or optimal methodologies that serve as a basis for formulating, executing, and overseeing an entity's procedures, regulations, or mechanisms. Frameworks provide organisations with a methodical approach to managing and mitigating cyber risks and ensuring a strong and adaptable security posture within cybersecurity.

The articulation/specification and identification notions are intricately linked to cyber resiliency. Articulating, or specifying, pertains to precisely defining a cyber resiliency plan's intended attributes, objectives, or consequences. On the other hand, identification entails the recognition of critical assets, susceptibilities, and plausible hazards that could affect an entity's digital framework. Integrating these procedures facilitates the creation of precise and efficient strategies for cyber resilience within institutions, guaranteeing their readiness and capacity to rebound from security breaches or interruptions.

Organisations must comprehend the distinction between security and resilience, the principles of taxonomy and frameworks, and the relationship between articulation/specification and identification to establish and execute effective cyber resiliency strategies in the constantly changing digital environment. Through these principles, entities can augment their capacity to endure and recuperate from cyber hazards, preserving their electronic resources and guaranteeing the uninterrupted continuation of their activities.

Judgmental heuristics are cognitive shortcuts strategies that individuals use to make decisions or judgments efficiently and swiftly (Ahmad, Shah, and Abbass 2020). These heuristics are often used when there is a lot of uncertainty or complexity and there is not enough or enough knowledge (Ahmad, Shah, and Abbass 2020). Even though these shortcuts can make it easier to make decisions, they can also lead to cognitive biases and mistakes because people may miss important information, rely on stereotypes, or let their feelings get in the way.

In the context of cyber resilience, judgmental heuristics can affect how people and organisations see cyber threats and react to them. For example, decision-makers may use

algorithms to determine how likely a cyber attack is, how to prioritise security investments, or how to implement mitigation strategies (Zeijlemaker et al. 2022). Some examples of judgmental heuristics that may be useful for cyber resiliency are:

1. The availability heuristic says that people can make decisions based on how easy it is to think of relevant examples. This can make people overestimate how likely certain online threats are, especially those that have been in the news recently or that the organisation has already experienced.

2. Anchoring heuristic: People may base their decisions on the first piece of information they hear, even if it has nothing to do with the choice they need to make. In terms of cyber resilience, this could mean that decision-makers put too much emphasis on certain security measures or technologies and miss out on other important parts of a well-rounded plan.

3. The representativeness heuristic says people can determine how likely something is based on its similarity to a known group or image. This can make people underestimate how likely new or unusual cyber threats are since they might not fit their ideas of a "typical" cyber attack.

4. Confirmation bias: People may look for or understand information in a way that backs up what they already think or believe. In terms of cyber resilience, this could cause decision-makers to ignore data that goes against what they think about how well their security measures work. This could give them a false sense of security.

Organisations that want to improve their cyber resilience need to understand how judgmental biases might affect how decisions are made. By being aware of these cognitive biases and implementing ways to reduce their effects, organisations can improve their ability to correctly assess cyber threats and respond to them, making them more resistant to cyber attacks.

Availability and continuity are cyber attacks in cybersecurity and information security, and they can be associated with various judgmental heuristics.

Availability refers to the accessibility and efficacy of information systems, services, and resources when authorised users request them (L. Kim, 2022). In other words, availability guarantees that systems and services are always operational and readily accessible to satisfy the needs of users and processes. Availability metrics include system reliability, response time, and the proportion of completed transactions or requests.

Conversely, continuity is the capacity to maintain operations and recover from disruptions, ensuring the uninterrupted delivery of vital services and functions. In the context of information security, business continuity planning and disaster recovery planning are essential components of continuity. For critical systems, continuity metrics may include recovery time objectives (RTOs), recovery point objectives (RPOs), and mean time to repair (MTTR) (Karie & Sikos, 2022).

Cognitive biases in decision-making can affect availability and continuity in the context of judgmental heuristics. For instance, when evaluating the availability of a system, decision-makers may rely on the availability heuristic, which involves estimating the probability of an event based on how readily relevant examples come to mind. This could result in an overestimation of system availability if recent successes are readily recalled or an underestimation if recent failures are more prominently remembered.

Similarly, optimism bias may influence decision-makers when planning for continuity, which is the tendency to underestimate the likelihood of adverse events and overestimate the ability to recover from them. This bias may result in insufficient investment in continuity measures, such as backup systems or redundant infrastructure, thereby increasing the organisation's susceptibility to disruptions.

To reduce the influence of subjective heuristics on evaluating and managing availability and continuity, it is essential to adopt systematic approaches and data-driven decision-making procedures. Some recommendations include the following:

1. Developing and implementing robust monitoring and measurement systems to watch availability and continuity metrics, supplying decision-makers with objective data.
2. Encouraging diverse viewpoints and collaborative decision-making to challenge assumptions and lessen the influence of individual cognitive biases.
3. Conduct periodic evaluations and audits of the availability and business continuity plans, incorporating lessons learned and best practices from industry benchmarks and standards.
4. Implementing scenario-based planning and simulation exercises to test and validate availability and continuity strategies, thereby aiding decision-makers in gaining a more realistic understanding of potential risks and obstacles.

Although judgmental heuristics can impact the evaluation and management of availability and continuity, recognising these biases and implementing systematic, data-driven processes can assist organisations in achieving more accurate evaluations and robust security strategies.

The Kepner-Tregoe (KT) methodology is a systematic approach to resolving problems and making decisions formulated by Charles Kepner and Benjamin Tregoe during the 1960s (Brightman et al., 1988). Within cyber resilience, this approach can bolster an organisation's capacity to preempt, endure, recuperate from, and adjust to cybersecurity obstacles. At the same time, the "Persona-Based" cyber resiliency assessment approach proposed in this study is based on the Kepner-Tregoe methodology.

The initial step in implementing the KT methodology entails conducting a situation appraisal, which encompasses evaluating an entity's cybersecurity stance (Brightman et al., 1988). Via this evaluation, entities can detect prevailing concerns, rank them according to their significance and immediacy, and acquire a more comprehensive comprehension of their cyber resilience capabilities and limitations. This procedure enables individuals to concentrate on mitigating the most crucial vulnerabilities and threats.

After conducting a thorough assessment of the situation, the problem analysis stage aids in identifying the underlying cause of each identified problem. Within cyber resilience, it may be necessary to scrutinise various elements, such as deficient security measures, insufficient employee education, or obsolete software. Identifying the root cause allows organisations to effectively address the underlying issue instead of solely addressing the symptoms.

Upon identification of the underlying causes, the subsequent step in the decision-making process entails the assessment of various alternative solutions for each issue. It is imperative that the process, as mentioned earlier, incorporates an evaluation of the potential benefits, costs, risks, and feasibility associated with each available option. Within cyber resilience, decision analysis entails evaluating various security technologies, training programs, or incident response strategies to determine the most suitable approach for enhancing the organisation's cybersecurity stance.

The Kepner-Tregoe technique culminates in the stage of potential problem analysis, which seeks to preemptively recognise and address any future problems that could emerge from the selected solutions. Regarding cyber resilience, this measure can aid organisations in predicting and getting ready for possible obstacles, such as novel attack vectors, technological obsolescence, or regulatory modifications. This guarantees that entities can adjust and react efficiently to the developing cybersecurity hazard environment.

To succinctly encapsulate the matter, utilising the Kepner-Tregoe methodology in bolstering cyber resilience endeavours enables us to bolster cyber resilience and rectify cybersecurity concerns. This facilitates the ability of individuals to arrive at better-informed and efficacious judgments, thereby enhancing their resilience during a constantly changing threat environment.

2.4 Existing Approaches For Measuring Cyber Resiliency

In cyber resiliency, various frameworks and approaches have to guide organisations in assessing and enhancing their ability to withstand and recover from cyber incidents. These frameworks offer unique perspectives and methodologies that can be tailored to an organisation's specific requirements and objectives. The following is a review of some widely recognised frameworks and approaches in the literature:

2.4.1 The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)

This is a comprehensive risk-based approach that enhances organisations' cybersecurity posture. The CSF comprises five core functions—Identity, Protect, Detect, Respond, and Recover—which can be customised to suit an organisation's needs and employed to evaluate cyber resiliency (Möller 2023; Roy 2020). Krumay, Bernroider, and Walser (2018) investigate the coverage of NIST functions in academic literature and identify gaps in the literature and the NIST framework. The study reveals imbalances in academic discourse and suggests that future research should focus more on detecting, responding to, and recovering from incidents. The authors also recommend extending the NIST framework to include topics such as natural disasters, monetary aspects, and organisational climate. This research provides valuable insights for evaluating cybersecurity-related risk management, which is becoming increasingly important for critical infrastructure providers (Krumay, Bernroider, and Walser 2018).

2.4.2 Factor Analysis of Information Risk (FAIR)

This is a quantitative risk analysis model that facilitates understanding, analysing, and quantifying information risk in financial terms (RiskLens, 2020). The FAIR model provides valuable insights into cyber resiliency by evaluating the potential impact of various cyber threats and the effectiveness of an organisation's risk management strategies. According to Ignat (2022), assisting upper-level management in making well-informed decisions concerning information security risks and investments by attaining reliable and uniform risk analysis outcomes. This research investigates the fundamental characteristics of a reliable methodology for analysing information risk. It evaluates FAIR's theoretical framework and structure and investigates its congruity with the NIST

Cyber Security Framework and ISO/IEC 27005. The text analyses multiple risk scenarios through the utilisation of FAIR. It further identifies potential challenges and factors that may facilitate the risk analysis. Additionally, the text proposes a concept for developing an information risk analysis tool for enterprises that prioritise risks and financial decision-making. This notion's practical implementation has ensured that the risk analysis process is expedited and streamlined by utilising specific input parameters stored in the database, which can be employed across various scenarios without needing expert consultation (Ignat 2022).

2.4.3 The Center for Internet Security (CIS) Critical Security Controls

CIS is a prioritised set of actions designed to improve an organisation's cybersecurity posture (CIS, 2020). These controls address multiple aspects of cybersecurity, including cyber resiliency, by providing a systematic approach to identifying, protecting, detecting, and responding to threats. Winarno, Yasin, Prasetyo, Rohman, Shihab, and Ranti (2022) evaluated the IT infrastructure security of PT. XYZ, an insurance company, encountered a malware attack in 2019. Utilising a qualitative methodology involving documentation and interviews, the investigation revealed that most of the control group, specifically 16 out of 20, surpassed the threshold value. This outcome suggests that the IT security infrastructure of the company is deficient. The study authors presented a set of 13 suggestions for enhancing organisational processes, which may serve as valuable insights for other entities, particularly within the insurance industry. Consequently, it has been confirmed that these measures are effectively implemented (Krumay, Bernroider, and Walser 2018).

2.4.4 NIST Special Publication (SP) 800-53

NIST Special Publication (SP) 800-53 offers comprehensive security controls and guidelines for federal information systems and organisations (NIST, 2013). The publication covers various controls related to incident response, contingency planning, and system recovery, which can be utilised to measure and enhance an organisation's cyber resiliency (Pillitteri et al. 2020). According to the study of Amiruddin et al. (2022), they focus on developing a cyber-risk management plan for the IT Unit of an organisation called XYZ. They use the NIST CSF as the main framework, CIS Controls v8 and NIST

SP 800-53 Rev 5 for defining controls and action recommendations. The research uncovers 42 risk scenarios, 12 of which are accepted and 30 are mitigated. Fourteen action recommendations are provided for the IT Unit to reach tier 3, based on 18 controls of CIS and 20 controls of NIST SP 800-53 Rev 5. This approach helps the IT Unit address current cyber risks and achieve a more formalised and documented cyber-risk management process (Amiruddin et al., 2021).

2.4.5 NIST SP 800-160 Vol. 2

NIST SP 800-160 Vol. 2 specifically focuses on cyber resiliency engineering, providing guidelines for designing, developing, and deploying resilient systems. This publication presents a systematic approach to assessing and improving cyber resiliency based on adaptive capacity, resistance, and recoverability (Ross et al. 2021). Mailloux et al. (2018)'s article delve into the engineering of secure and resilient systems by examining security strategies and principles presented in Appendix F of NIST SP 800-160. The paper briefly introduces systems security engineering and describes the strategies and principles outlined in NIST SP 800-160 Appendix F. The study maps abstract security strategies to concrete security principles, facilitating implementation, tracing, and testing. The research is part of a series aiming to help developers, owners, and operators understand and apply a rigorous Systems Security Engineering approach. Future work will focus on efficiently applying these principles, exploring their applicability to cyber resiliency, and identifying suitable technical performance measurements and criteria (Mailloux, Beach, and Span 2018).

2.4.6 The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)

ISO/IEC have jointly developed the ISO/IEC 27000 series of standards for information security management (ISO/IEC, 2018). These standards furnish a comprehensive framework for implementing and managing information security controls, encompassing aspects related to cyber resiliency. In the article "Comparative Study of Ontologies Based on ISO 27000 Series Security Standards", the authors deeply analyse six main ontologies that stress how to use the ISO/IEC 27000 series of security standards. We look at these ontologies in terms of their goals, the security ideas they cover, and how they use ISO 27000 features. The study provides a thorough comparison, considering the specific

ISO/IEC 27000 standard used, any missing concepts, the integration of other standards and best practices, the method used, and the validation and evaluation of the security ontology.

The study aims to give security decision-makers useful insights and suggestions to help them choose an ontology that meets their security needs. Also, the study is a useful resource for researchers and practitioners who need to build security frameworks that include security ideas and ISO 27000 features (Meriah and Rabai 2019).

The authors discuss the importance of having a more unified security ontology that includes many standards from the ISO 27000 series and covers all important security ideas. Such a theory would follow a clear method and ensure that the evaluation and validation process is thorough. The paper says future studies should focus on the suggestions, especially in security risk management and ISO 27000 series security standards based on ontology. As another possible direction for future work, creating a new ontology that describes a specific security risk analysis model for information systems could be looked into (Meriah and Rabai 2019).

In summary, the literature on cyber resiliency presents an array of frameworks and approaches organisations can employ to assess and enhance their ability to withstand and recover from cyber incidents. Researchers and practitioners can choose from these frameworks or adopt a combination, depending on their needs and goals.

2.5 Zero Trust Philosophy And Its Relevance To Cyber Resiliency

2.5.1 Applying maritime warfare insights: zero-trust, multi-factor authentication, and cyber resiliency in the digital age - a case study from the HMAS Sydney-Kormoran encounter

The zero-trust paradigm and multi-factor authentication (MFA) have garnered considerable attention in cybersecurity, offering a resilient structure for enterprises to safeguard their essential resources. Cyber resilience is crucial for organisations to maintain their operations in the face of cyber threats and attacks. The historical incident during the Second World War involving the German auxiliary cruiser Kormoran and the

Australian light cruiser HMAS Sydney is a valuable context for comprehending these principles and their pertinence in modern-day cybersecurity.

A naval confrontation of significant intensity occurred on November 19, 1941, between the German auxiliary cruiser Kormoran and the Australian light cruiser HMAS Sydney in the waters of the Western Australian coast. Under the leadership of Fregattenkapitän Theodor Detmers, the Kormoran employed a Dutch merchant vessel guise to circumvent detection by hostile military entities. Upon the HMAS Sydney's approach to the Kormoran, led by Captain Joseph Burnett, the latter disclosed its identity and attacked the former, catching the Australian vessel off guard. The HMAS Sydney and Kormoran vessels were ultimately destroyed, resulting in the unfortunate loss of all 645 crew members on the former and 82 crew members on the latter.

On a cloudy day off the coast of Western Australia, the German auxiliary cruiser HSK Kormoran sailed without being seen because it was dressed as a cargo ship and kept its weapons hidden. As it moved forward, Kormoran's captain, Detmers, saw a warship on the horizon. It was the Australian light cruiser HMAS Sydney, and it was coming up fast. Sydney flashed the signal NNJ ("You should make your signal letters") from a projector to find out who was on the mystery ship. Other ships sent their names using different radio signals and coloured flags.

Even though Kormoran was smaller and less well-equipped than Sydney, it kept its secret by pretending to be the innocent merchant ship "Straat Malacca." By doing this, the ship could get through the water safely by pretending to be legal. "PKQI," the code letter for the Dutch freighter Straat Malacca, was Kormoran's answer to Sydney's message. As the two ships got closer, Kormoran sent a "QQQQ" signal to make Sydney think it had seen a strange ship. The goal was to confuse Sydney and keep up the appearance that it was a good ship.

Sydney got a weak and distorted form of the message, so she kept asking Kormoran questions. When asked where the message was going, she was told, "Batavia." Even though the Dutch freighter said it was safe, the Australians did not believe it. At the time,

ships could be proven to be whom they said they were by asking for the last four characters of their code after learning their declared name. Sydney sent the second and third numbers of Straat Malacca's secret callsign "IIXP" as "IX" to verify it.

Since Kormoran did not know the secret code and thought "IX" meant "hurricane," he did not give the right answer. This made Sydney suspicious, so the ship moved closer to Kormoran, accidentally putting it in the Germans' line of fire. Seeing an opening, Kormoran put up a German flag, showed off its weapons, and struck the Australians without warning. Sydney was caught off guard and had no way to protect itself, so it finally sank.

Security measures were not taken during this historical event, and important steps were skipped. Even though Sydney was a warship, it did not use all of the protection measures it had. Some of the most important things that Sydney should have done that have to do with current cybersecurity practices are: - Cargo ships were not allowed in the area; the Access Control List (ACL) was not used.

HSK Kormoran hid its flag so that no one would know who it was; no one knew who it was.

Multi-Factor Authentication (MFA) did not work, so HSK Kormoran could not finish the secret code of Straat Malacca.

This event shows that the most important thing to protect, no matter what time it is, is "identity." It shows how important it is to have methods that can adapt to the day's technology and how the Zero Trust principles can be used even in this situation. In this way, the Zero Trust Architecture is an example of a security method that looks at the whole picture and is not limited by time or place.

The unfortunate incident can be a warning for institutions that aim to incorporate zero-trust and cyber resilience approaches in their cybersecurity endeavours. HMAS Sydney's failure to verify the identity and intentions of the Kormoran before approaching it can be interpreted as a deviation from the Zero-Trust principles. These principles emphasise the

importance of ongoing verification of identity and access before granting resource access. On the other hand, Kormoran's deception underscores the significance of implementing strong authentication protocols, such as MFA, that necessitate multiple means of verification to authenticate the authenticity of an entity.

The zero-trust principle posits that entities, regardless of their origin, should not be automatically trusted by organisations. Instead, every access request should be verified. The application of this principle can be observed in the decision-making process of Sydney during the Sydney-Kormoran encounter. If Sydney had implemented a zero-trust approach, it would have taken measures to authenticate the identity and motives of the Kormoran prior to engaging with them. This could have conceivably prevented the catastrophic consequences of their interaction.

Multi-Factor Authentication (MFA) is an essential element of the Zero-Trust framework, which mandates that users provide multiple forms of verification to gain access to sensitive resources. Regarding the naval engagement, it could be suggested that Sydney could have implemented a similar strategy by requiring the Kormoran to provide various means of identification, including but not limited to visual confirmation, radio communication, and scrutiny of vessel documentation. Implementing multi-factor authentication (MFA), protocols could have enabled Sydney to detect Kormoran's deceitful actions and prevent the ensuing altercation that ultimately resulted in its demise.

The notion of "cyber resilience, " pertains to an organisation's capacity to sustain its operations in the face of cyber threats and attacks, is equally applicable at the current historical juncture. While the engagement between Sydney and the Kormoran occurred in the tangible realm, applying the tenets of cyber resilience to the strategies implemented by both vessels throughout the conflict is feasible. Despite incurring considerable harm, the Kormoran's capacity to endure the attack from Sydney can be regarded as an illustration of resilience in adversity.

The resilience exhibited by the Kormoran can serve as a valuable lesson for organisations seeking to enhance their cybersecurity strategies. Organisations can fortify their security

measures by embracing a proactive stance towards cybersecurity, enabling them to sustain their operations in the face of potential threats or attacks. Implementing cyber resilience strategies, such as redundancy, segmentation, and continuous monitoring, can enhance an organisation's ability to detect and respond to threats more efficiently.

The encounter between Sydney and Kormoran highlights the repercussions of inadequate security measures, which resulted in the unfortunate loss of lives on both vessels. Modern cybersecurity presents organisations with progressively intricate threats, necessitating a comprehensive strategy to safeguard their crucial assets and infrastructure. By assimilating insights from this significant occurrence, entities can enhance their comprehension of the criticality of deploying zero-trust, multi-factor authentication, and cyber resilience tactics.

To conclude, the interaction between the German auxiliary cruiser Kormoran and the Australian light cruiser HMAS Sydney in the context of the Second World War provides significant perspectives on zero trust, multi-factor authentication, and cyber resilience. The adverse result of the conflict serves as a poignant indication of the significance of sturdy security protocols and the necessity for continuous authentication of identity and entry.

Organisations can safeguard themselves against potential deception, similar to the incident involving HMAS Sydney, by adopting the Zero-Trust philosophy, which mandates the continuous authentication of all access requests. Deploying multi-factor authentication (MFA) can furnish an extra layer of security by requiring multiple modes of identification to avert illegal entry to critical assets.

In addition, implementing Cyber Resiliency tactics can aid entities in sustaining their operability and safeguarding their essential resources amidst challenging circumstances. By examining past occurrences such as the Sydney-Kormoran incident, entities can enhance their cybersecurity stance, fortifying their valuable assets and guaranteeing sustained viability within a more hostile digital environment.

2.6 Zero Trust Philosophy

The zero-trust paradigm asserts that an enterprise must not automatically place trust in any entity, whether internal or external and must instead authenticate before authorising access (Rose et al. 2020). The cybersecurity strategy in question incorporates many fundamental principles, such as "micro-segmentation," "least privilege access," and the "Pillars of Zero Trust Architecture."

Following a successful infiltration of an organisation, attackers commonly employ a strategy referred to as "lateral movements" to extend their level of control; the zero-trust paradigm provides a security approach that specifically tackles this scenario (Shore, Zeadally, and Keshariya 2021). Organisations can limit the horizontal progression of potential attackers who have gained access by implementing micro-segmentation, which is one of the fundamental principles of the zero-trust model (Simpson and Foltz n.d.).

During the initial phases of digitalisation, institutions frequently utilised a "flat network" configuration, granting unrestricted access to all documents and resources to all organisation members without access control mechanisms (Wagner et al. 2017). Nonetheless, this methodology proved unfeasible because confidential information, such as personally identifiable information (PII), became readily available to everyone. In order to address this matter, entities commenced implementing a network architecture known as "micro-segmentation" (Basta et al. 2022).

Microsegmentation offers security teams precise management, guaranteeing that only appropriate personnel can obtain relevant resources. Micro-segmentation can be deployed across three classifications: agent-based, network-based, and native cloud (Klein 2021).

The relationship between zero trust and micro-segmentation frameworks can be established in individual access privileges and verification. The policy commonly referred to as "Least Privilege Access" is an intermediary between the abovementioned structures. This policy resembles the Zero Trust policy but also displays notable

distinctions. The zero-trust model posits that access to a given entity should not be granted until its level of trustworthiness has been verified. The Zero Trust model is distinct from the principle of least privilege access in that it mandates the provision of trust prior to the conferment of any access rights.

Within micro-segmentation architecture, the principle of least privilege is upheld concerning user access, whereby users are granted only the essential access required to perform their designated tasks. The minimisation of security risks is achieved by implementing granular access privilege restrictions for individuals. As an illustration, the adverse effects of an apparent security violation can be restricted to a specific set of tasks.

The implementation of micro-segmentation facilitates the application of the zero-trust principle by introducing a highly detailed level of segmentation. The network is partitioned based on discrete workloads, with each resource linked to security policies meticulously calibrated by the respective workload. This principle is considered a fundamental element of the Zero Trust Architecture.

2.7 Literature Gaps

One of the most significant gaps in the literature on cyber-resiliency is the lack of comprehensive frameworks that effectively combine persona-based and risk-based measures. Contemporary scholarly investigations tend to primarily concentrate on two distinct methodologies: risk-based tactics that prioritise the detection and alleviation of potential hazards and persona-based strategies that emphasise the duties and obligations of personnel within a corporation.

Ahmad Maulana Fikri, Lovinta Happy Atrinawati, and Muhammad Gilvy Langgawan Putra (2022) conducted a study on evaluating cyber resilience practices at University XYZ. The study employs ten Cyber Resilience Review (CRR) assessment domains. The Critical Infrastructure Cyber Community Resilience (CRR), formulated by the Department of Homeland Security (DHS), is an assessment mechanism to measure the efficacy of cybersecurity protocols and service continuity among critical infrastructure proprietors and operators. The research methodology involves conducting interviews

with process owners and employing Maturity Indicator Levels (MILs) to assess the level of maturity of cybersecurity processes in the ten domains.

The assessment findings indicate that University XYZ has not attained Maturity Indicator Level (MIL)-1 in any of its domains, and the performance percentage for each CRR domain falls below 100%. The result above can be ascribed to inadequate implementation of procedures and incomplete data management protocols at the university. The researchers formulated recommendations for enhancing each domain, prioritising organisational objectives, business objectives, and resource feasibility to tackle these concerns. By implementing these suggested measures, University XYZ can augment its cyber resilience and guarantee the optimal operation of its systems, even in the face of potential cyber threats (Fikri, Atrinawati, and Putra 2022).

In this research, a noteworthy aspect of the methodology involves the organisation initially undergoing a self-assessment procedure. In the context of persona and risk-based cyber resilience assessment, the pertinent organisation completes a self-assessment process before conducting risk and persona audits. While there may be a resemblance, this study does not encompass persona-based and risk-based approaches.

Also, the article "Cyber Resilient Behavior: Integrating Human Behavioral Models and Resilience Engineering Capabilities into Cyber Security" by Rick van der Kleij and Rutger Leukfeldt presents a novel framework of cyber resilience that combines models from resilience engineering and human behaviour (van der Kleij and Leukfeldt 2020). The study highlights the significance of assessing cyber resilience and its potential role in shaping efficacious behaviour modification initiatives.

The study employed a methodology that entailed the creation of a conceptual framework that delineated resilient behaviour, which was subsequently translated into a questionnaire referred to as the Cyber Resilient Behavior Questionnaire. The survey evaluates the staff's aptitude, circumstances, and drive to execute four universal resilience functions: anticipation, monitoring, response, and learning. The instrument was refined

through expert feedback and validity testing, followed by a pilot study involving 56 small and medium-sized enterprises (SMEs) in the Netherlands.

The preliminary investigation indicated that nearly 50% of small and medium-sized enterprises (SMEs) had encountered at least one cyberattack within the preceding 12-month period, with phishing and viruses being the most frequently cited attack types. The collective cyber resilience score of these small and medium-sized enterprises (SMEs) was deemed suboptimal to moderate, with the most noteworthy scores observed in reacting to cyberattacks and the least notable in assimilating lessons from such attacks. The study's findings suggest that, while the small sample size limited further analyses, there is potential for enhancing cyber resilience among small and medium-sized enterprises (SMEs).

To sum up, the framework offers organisations a diagnostic instrument to enhance the human facets of cyber resilience and equip themselves for upcoming cyber hazards. The utilisation of the Cyber Resilient Behavior Questionnaire facilitates a thorough evaluation of an entity's cyber resilience through the inclusion of personnel from diverse hierarchical and operational backgrounds. Subsequent investigations should encompass more extensive participant pools, encompass personnel from diverse hierarchical strata, and authenticate the framework and tool across disparate commercial domains.

Nonetheless, this investigation does not provide unequivocal findings concerning cyber resilience in organisations. By evaluating personas and risk-based cyber resilience, the study identifies the deficiencies in information security measures within organisations and introduces cyber resilience as a quantifiable notion by assigning a score out of 100 to organisations.

The current corpus of knowledge lacks a comprehensive comprehension of the integration of these two methodologies in order to establish a resilient and flexible cyber-resiliency plan. Addressing this gap is essential for developing more effective methods that capitalise on the strengths of both risk- and persona-based approaches, ultimately

helping organisations better protect their digital assets and respond to the ever-evolving landscape of cybersecurity threats.

The extant literature on cybersecurity exhibits a unique constraint in its inadequate emphasis on human factors and their pivotal function in promoting cyber-resiliency. Although technical measures are unquestionably necessary, it is crucial to acknowledge that an organisation's staff members' behaviour, attitudes, and comprehension significantly impact its cybersecurity posture. This underscores the significance of implementing a persona-based strategy that considers the distinct characteristics, duties, and functions of personnel within a company. Organisations can enhance cyber-resiliency by developing tailored and efficacious strategies that enable employees to contribute to cybersecurity by comprehensively comprehending diverse personas and their distinct cybersecurity requirements. Integrating persona-based controls within cybersecurity frameworks can augment the comprehensive efficacy of risk management by attending to the human factor and cultivating a culture that prioritises security awareness. By addressing the gap, as mentioned earlier in the existing body of literature and highlighting the importance of persona-based controls, scholars can make a valuable contribution towards achieving a more all-encompassing comprehension of cyber-resiliency. This, in turn, can facilitate the development of more resilient and adaptable cybersecurity tactics.

In this research, the Persona-Based methodology within the Zero-Trust security framework synergises the foundational Zero-Trust principles with the concept of personas. This approach broadens the "untrusted users" notion, using personas to ascertain the appropriate level of access for each user within an organisation, considering their role, responsibilities, and access necessities.

3. METHODOLOGY

3.1 Description and Development of Cyber Resiliency Control Matrices

The present study utilises a dual framework approach that integrates a Risk-Based Cyber Resiliency Ability Control Kit and a Persona-Based Zero-Trust Cyber Resiliency Ability Control Kit to evaluate an organisation's cyber resilience. Integrating two frameworks offers a thorough and multifaceted methodology for assessing an entity's ability to endure cyber risks and respond efficiently to cyber events.

The Risk-Based Cyber Resiliency Ability Control Kit is a structured approach that employs quantitative methods to evaluate an organisation's capacity to handle, alleviate, and recuperate from cybersecurity hazards. The process centres on a methodical recognition, assessment, and ranking of hazards, considering the consequences and the probability of their manifestation. Adopting a risk based approach is important for organisations as it facilitates their comprehension of the threat landscape and enables them to allocate resources in an efficient risk mitigation and incident response.

The integration of Zero-Trust security principle Integrating of personas is a key feature of the Persona-Based Zero-Trust Cyber Resiliency Ability Control Kit. The approach expands upon conventional security protocols by classifying users according to their designated roles, responsibilities, and access prerequisites. This affords enterprises a more detailed oversight of network resource accessibility and bolsters their ability to address potential security breaches promptly.

Implementing a security frame addresses potential security breaches promptly in organisational tasks (Alotaibi, Furnell, and Clarke 2017). The model entails a comprehensive documentation and procedural regimen, which may demand significant development, implementation and maintenance resources. It also necessitates a cultural change within the organisation, where employees must grasp the significance of security and undergo training on security policies and procedures.

Organisations may need technical and infrastructural modifications to align with the model's requirements, which can be time-consuming and cost prohibitive. Ensuring compliance necessitates reevaluations and audits, which can be arduous and resource intensive. Furthermore, the need for continuous improvement of the security posture in response to the dynamic threat landscape necessitates frequent updates to security policies, procedures, and technologies, making it a complex and ongoing process.

However, considering the situation in the mentioned structure, the determined at the most basic level is; the need to re-architect the network infrastructure to support the zero-trust and risk-based model. This can be a significant undertaking, as it requires organisations to rethink their entire approach to network security and redesign their networks to support the zero-trust network architecture model (Teerakanok et al. 2021). This risk-based and persona-based model can offer a strong start to compliance. This other information security and IT governance standards.

Both of these frameworks have been devised to furnish a quantifiable rating, on a scale of 0 to 100, that reflects the resiliency exhibited by the organisation. As mentioned earlier, the score serves as a numerical depiction of the current level of cyber resilience score, as mentioned earlier action, and it also functions as a standard for monitoring advancements made over a while.

Moreover, the results of utilising the pair above while assessments are closely associated with onions outlined in establishing pair security and IT governance protocols. The process above furnishes audited entities with specific and feasible suggestions for enhancing their operations. As mentioned above, the process rarely determines the standards they must consult to rectify identified shortcomings and deviations. The distinctive characteristic of the methodology reinforces its practical significance and suitability, rendering it a valuable instrument for augmenting cyber resilience in actual scenarios.

3.2 Research Design

Through a set of audit questions, this study aims to demonstrate the compatibility of an organisation's zero-trust and cyber resilience practices with world-class standards on a persona and risk basis. Although this set of ability control questions may resemble an audit, it should not be considered a certification process. Instead, it gives the organisation a score of 100, indicating the degree of alignment between its zero-trust and cyber resilience practices and world-class standards. The examination constitutes a gap analysis, evaluating existing resources and outlining a strategy for proper implementation by leveraging these resources.

In order to accurately assess the level of compatibility, a set of questions was designed to gather relevant information, and the data collection process is critical to the success of this study, as it forms the foundation of the analysis.

In addition to the questionnaire, vital organisational stakeholders were interviewed for further information. The in-person or via telecommunication interviews were structured to cover the same topics as the questionnaire.

3.3 Ethical Considerations

Data confidentiality was a cornerstone principle upheld throughout this research process. All collected information was treated with the utmost respect for privacy, adhering strictly to relevant ethical and legal guidelines, thereby safeguarding the integrity of any personal information involved.

Names of organisations and individuals who participated in the study were anonymised to maintain the data's confidentiality and to ensure their anonymity. Such anonymisation protects the participants' identities while preserving the utility and integrity of the data collected.

The research protocol also required organisations to provide informed consent before participation, underscoring the ethical commitment to transparency and respect for participants' autonomy. As part of the protocol, organisations were provided with a

consent form clearly outlining the purpose of the research, how their data would be used, and the measures in place to protect their confidentiality. Acknowledging the receipt and understanding of this information, participating organisations signalled their agreement to participate by returning the signed consent form. A sample of this consent form is included in Appendix A.

3.4 Audit Questions and Their References

In instances where an organisation demonstrates non-compliance with a specific control, it is likely that it similarly fails to meet the corresponding clauses of the standards that the respective control questions reference. This observation arises from a logical extrapolation, given that these control questions are, in essence, derivations and implementations of these standards. Thus, non-adherence to control often signals non-conformity with the underpinning standard.

Therefore, in the audit report furnished to the organisation upon the culmination of the assessment, a comprehensive perspective on the deficiencies exhibited by the organisation is also provided. This includes immediate control non-compliance and a broader overview of the standard-based clauses potentially not being fulfilled. Consequently, the audit report identifies the immediate areas of concern and guides the organisation towards a holistic improvement of its compliance landscape based on established standards.

Each question references these standards, frameworks, laws, and benchmarks;

- ISO/IEC 27001; is an international standard that outlines best practices and requirements for information security management systems (ISMS). It systematically manages and protects sensitive information, including data and intellectual property, through risk management processes and security controls.
- NIST Cybersecurity Framework (CSF); is a set of guidelines and best practices developed by the National Institute of Standards and Technology (NIST) to support organisations in managing and reducing cybersecurity risk. It provides a

common language and a flexible, repeatable approach to cybersecurity that can be tailored to meet the unique needs of any organisation.

- NIST SP 800-53; is a publication from NIST that provides security and privacy control guidelines for federal information systems and organisations. It provides a catalogue of security controls and objectives organisations can use to develop a comprehensive security program and comply with federal regulations.
- NIST SP 800-34; is a publication from NIST that provides guidelines and recommendations for developing a Contingency Plan for federal information systems. It provides a step-by-step approach to help organisations prepare for and respond to unexpected events that could disrupt normal operations, such as cyber-attacks, natural disasters, or power outages.
- NIST SP 1800-35; is a publication by NIST that provides guidelines for disaster recovery and business continuity planning for information systems. The publication provides practical recommendations for organisations to develop, implement, and maintain an effective disaster recovery and business continuity program to ensure the availability of critical information systems and data.
- COBIT 5; Control Objectives for Information and Related Technology is a framework for enterprise information and technology governance and management. It provides a comprehensive set of guidelines, processes, and best practices for evaluating and improving an organisation's IT governance and management practices.
- COBIT 2019; is a framework for governance and management of enterprise information and technology (I&T), which provides a comprehensive set of best practices, guidance and templates to help organisations manage the end-to-end life cycle of I&T. It provides a comprehensive set of practices and guidelines for all aspects of enterprise I&T governance, management and operations. It is widely used for IT governance, risk and compliance management.
- ITIL; Information Technology Infrastructure Library is a framework that provides a set of best practices for managing and delivering IT services. It covers the entire service lifecycle, from strategy and design to operation and continual service improvement. Organisations widely adopt ITIL worldwide to help align their IT services with business needs and improve overall service quality.

- PCI DSS, Payment Card Industry Data Security Standard, is a comprehensive set of security standards aimed at ensuring the secure handling of credit card information by companies that accept, process, store, and transmit credit card data. The standard aims to provide a structured approach to preventing security threats such as credit card fraud, hacking, and other vulnerabilities, thus promoting a secure environment for handling sensitive payment card information.
- SOC 2, System and Organization Controls 2, is a set of security standards and guidelines by the American Institute of Certified Public Accountants (AICPA) to assess a service organisation's security controls and practices. It assures customers and stakeholders that the service organisation has implemented sufficient security controls to protect customer data and information systems.
- GDPR; The General Data Protection Regulation is a regulation in European Union law that aims to protect privacy and data protection rights. This regulation, enacted on May 25, 2018, superseded the 1995 EU Data Protection Directive. The GDPR establishes rigorous standards for organisations that handle the personal data of EU citizens and imposes substantial penalties for non-compliance.
- CIS Critical Security Controls; Center for Internet Security Critical Security Controls is a prioritised set of actions organisations can take to improve their cybersecurity posture and reduce the risk of cyber attacks. It is a globally recognised framework outlining 20 critical controls organisations should implement to secure their systems and data better.
- CSA Cloud Control Matrix; is a security framework for cloud computing developed by the Cloud Security Alliance. It provides a set of security controls and guidelines to help organisations evaluate and assess the security of cloud providers and services and to ensure the confidentiality, integrity, and availability of data in the cloud.
- HIPAA; The Health Insurance Portability and Accountability Act is a federal statute in the United States that outlines standards for maintaining the confidentiality and security of personal health information in healthcare settings. This law mandates that entities covered under HIPAA must establish administrative, physical, and technical measures to preserve the privacy and security of electronically protected health information (ePHI).

- FISMA, Federal Information Security Modernization Act, is a US law that mandates federal agencies to establish, document, and implement a comprehensive framework to protect their information and information systems from cybersecurity threats. It provides guidelines for federal agencies to manage their information security risks and to comply with security standards established by NIST.
- FERPA, Family Educational Rights and Privacy Act is a US federal law protecting student educational records' privacy. It requires educational institutions that receive federal funding to maintain the confidentiality and security of student records and regulate the release of this information to third parties.
- GLBA; Gramm-Leach-Bliley Act, a US federal law requiring financial institutions to protect their customers' personal information. The law sets standards for safeguarding sensitive data, including privacy notices and security measures, and requires financial institutions to ensure customer data security and confidentiality.
- SOX; Sarbanes-Oxley Act, a US federal law enacted in 2002 that sets standards for public company accounting and financial reporting to protect investors from fraudulent corporate financial reporting. It also established the Public Company Accounting Oversight Board (PCAOB) to oversee the activities of auditors of public companies.

3.5 Risk-Based Cyber Resiliency Assessment Kit

The “Risk-Based Cyber Resiliency Assessment Kit,” as proposed in this study, offers a distinct methodology that accommodates the variability in organisational size and structure. This framework recognises that the volume and nature of questions applicable to an enterprise of large scale may not be directly applicable to smaller entities. This is predominantly because intricate details regarding information security, which are pertinent to large corporations, may bear a different weight in smaller establishments. Thus, the size and structure of an organisation significantly determine the salient parameters of its cyber risk assessment.

Moreover, this kit necessitates a collaborative approach involving the participation of the organisation's Information Security or IT Director. Each query within the assessment is meticulously evaluated and scored on a scale of 1-5. These scores are assigned based on four critical metrics, Confidentiality, Integrity, Availability, and Likelihood or Effectiveness, contingent upon the context of the problem. Where confidentiality pertains to the preservation of information privacy and the prevention of unauthorised disclosure, safeguarding confidential data usually entails the implementation of access controls, encryption, and various other security measures. Where integrity pertains to the credibility and dependability of data, precautions are implemented to guarantee that data is not modified or eradicated in an unapproved or unforeseen way. The task at hand pertains to upholding information's coherence, precision, and reliability throughout its complete duration. Where availability guarantees that authorised users can access information when required, ensuring its accessibility. The task pertains to preserving dependable information accessibility, commonly achieved through implementing backup systems and resilient infrastructure that can effectively recuperate from malfunctions. The CIA triad, a fundamental concept in information security, traditionally comprises confidentiality, integrity, and availability. However, it is imperative to note that likelihood or effectiveness, although not traditionally included in the CIA triad, is a critical factor that must be considered in risk assessment methodologies.

Likelihood pertains to the probability of a potential threat exploiting a vulnerability, which may lead to an unfavourable impact on the organisation. The analysis considers various elements, including the capacity of the threat, the degree of threat presence, and the presence of vulnerabilities.

Effectiveness refers to the degree to which the controls implemented by an organisation can manage, mitigate, or prevent potential threats. The evaluation process assesses the adequacy of control design, implementation accuracy, and conformity to intended operations.

The concepts mentioned above serve as the fundamental basis for any approach to managing risks associated with information security and are crucial for comprehending and enhancing an entity's ability to withstand cyber threats.

By doing so, the risk score corresponding to each question for the organisation is precisely calculated.

From this perspective, each audit becomes a unique and custom-tailored evaluation conducted in alignment with the distinct features of the audited organisation. Such an approach enables a more robust and personalised understanding of the organisation's needs, thus ensuring a nuanced and precise appraisal of its cyber resiliency posture. This strategy, in turn, paves the way for actionable insights that cater to the organisation's specific requirements, significantly enhancing its overall cyber resiliency framework.

Several values are needed in the formula to calculate the Risk-Based Cyber Resiliency score: Control's Risk Score, Number of Audit Questions, Maximum Risk Score of the Organization, Control-Based Risk Score, and Organisation's Actual Risk Score.

When calculating the organisation's overall cyber resiliency score, only 70% of this assessment's score is included due to the question content and amount of the risk-based assessment.

In Appendix B, one ability control question sample is given for each ability control section, a similar risk analysis section is given, and also a pool of all questions used in this assessment kit is given; in an holistic view, an example of a risk-based assessment kit can be observed in Appendix B.

3.5.1 Control's Risk Score (CRS):

This value represents a risk score value for each control question. It is rated out of five; as this score determines the risk value of each control question, it significantly impacts the cyber resilience score that the organisation will receive out of 100. Two different

points are obtained from this value; The first is the Maximum Risk Score of the Organization (MRSO), and the other is the Organization's Actual Risk Score (OARS).

This risk score is derived from a combination of effectiveness scores according to the three main elements of information security - confidentiality, integrity and availability, and the likelihood or context of the issue.

$$CRS = LE \cdot (C + I + A) \quad (3.5.1.a)$$

To clarify the mentioned statement, let us consider the components of the Control's Risk Score (CRS) - Likelihood or Effectiveness (LE), Confidentiality (C), integrity (I), and Availability (A). Each element in the CRS formula can hold a maximum value of 5.

When these maximum values are inserted into the formula, the highest possible score for CRS is 75 (derived from $LE \cdot (C+I+A) \cdot 5 = 5 \cdot (5+5+5) \cdot 5 = 75$). This maximum value, however, is not easily digestible in the context of the control kit, as the scores are typically interpreted on a scale of 1 to 5.

A normalisation process is carried out to make the scores more understandable and fit them within the familiar scale. The calculated CRS is multiplied by a normalisation factor of 5/75. This operation brings the score within a range of 0 to 5, making it more comprehensible and easier to integrate with the control kit's established scale.

The normalisation operation ensures that the CRS fits within the expected scoring range, rendering it more useful and easily comprehended in an organisational context.

$$CRS = \frac{LE \cdot (C + I + A) \cdot 5}{75} \quad (3.5.1.b)$$

3.5.2 Number of Audit Questions (naq)

In the main formulation, this value is expressed as “naq”. The number of audit questions refers to the number of questions to be answered for a relevant control question.

3.5.3 Maximum Risk Score of the Organization (MRSO)

The Maximum Risk Score of the Organization (MRSO) is a cumulative measure of all potential organisational risks. It calculates the risk scores for all control questions within the evaluation kit.

Each control question has an associated Control’s Risk Score (CRS), which quantifies the level of risk it represents. By adding up these individual CRS values for all control questions, we get the MRSO.

In simpler terms, consider each control question a potential risk point for the organisation. The MRSO is the sum of these risk points, giving us a ‘worst-case scenario’ total risk score. This score represents the organisation's highest possible risk exposure based on the assessment's control questions.

$$MRSO = \sum_{k=1}^{naq} CRS_k \quad (3.5.3.a)$$

3.5.4 Control-Based Risk Score (CBRS)

The Control-Based Risk Score (CBRS) is a measure that reflects the risk score of each control question with the organisation’s current situation. It uses the Control’s Risk Score (CRS), which is a score assigned to each control question indicating its potential risk, but adjusts it based on whether the organisation complies with the control.

In simpler terms, each control question has a risk score (the CRS). However, if an organisation has already met the requirements of that control question, then the actual risk to the organisation from that control is effectively null. On the other hand, if the

requirements of that control question are not met, then the organisation faces the full risk as indicated by the CRS.

This is done by introducing a binary variable, 'A', based on the organisation's answer to the control question. If the answer is 'yes' (meaning the control is in place), 'A' is set to 0. If the answer is 'no' (meaning the control is not in place), 'A' is set to 1.

```
If Answer = "yes" Then
  Set variable A = 0
Else If Answer = "no" Then
  Set variable A = 1
End If
```

The CBRS is then calculated by multiplying the CRS by 'A'. Therefore, if control exists (A=0), the CBRS is 0 regardless of the CRS. If a control is not in place (A=1), the CBRS equals the CRS. This way, the CBRS provides a more tailored risk score that reflects the actual risk exposure of the organisation for each control question.

$$CBRS = CRS . A \quad (3.5.4.a)$$

3.5.5 Organisation's Actual Risk Score (OARS)

The Organization's Actual Risk Score (OARS) is the total risk score the organisation currently faces based on the controls it has yet to implement.

In other words, each control questions the organisation answers with a "no" (indicating that it does not have that control in place) carries a certain risk, as measured by the Control-Based Risk Score (CBRS). These individual CBRS scores for each unmet control are added to find the actual risk for the organisation.

The OARS is the sum of all the risk scores of the control questions where the organisation's answer was "no". This score represents the actual risk exposure of the organisation based on the controls it currently lacks.

It is the sum of all risks the organisation faces from not having certain controls.

$$ARS = \sum_{k=1}^{naq} CBR S_k \quad (3.5.5.a)$$

3.5.6 Organisations Risk-Based Cyber Resiliency Score (RB):

The RB score is obtained by subtracting the Organization's Actual Risk Score (OARS) from the Maximum Risk Score of the Organization (MRSO).

However, since the value obtained due to this arithmetic will not mean a meaningful result when it is not indexed to any score, it has been standardised over 100.

$$RB = \frac{MRSO - OARS}{MRSO} \cdot 100 \quad (3.5.6.a)$$

3.6 Persona-Based Zero-Trust Resiliency Assessment Kit

The Persona-Based Zero-trust Resiliency assessment kit is also a framework, a system, or a method that measures an organisation's security posture in terms of its ability to protect sensitive data and systems based on Zero-trust principles. The framework evaluates the organisation's security posture by assessing the resiliency of each persona, which is a specific role or user within the organisation.

Every organisation encompasses a diverse range of personas, which can refer to either a natural person or a non-person entity (NPE), such as an integration/service user or a scan user conducting compliance checks in various databases. When personas are associated with a natural person, they are classified as person entities (PE). In this context, the characterisation of personas may vary among sectors and organisations. Hence, establishing a comprehensive organisational chart is a fundamental requirement for conducting a Persona-Based Zero-Trust assessment.

In a Persona-based approach to the Zero-Trust system, each user is assigned one or more personas, which are used to determine the access level to network resources. For example,

a user who is assigned the persona of “system administrator” would have a higher level of access to network resources than a user who is assigned the persona of “guest” (Prabhu Kavın et al. 2020).

This approach presents specific elements from various security frameworks, benchmarks, and standards to serve as a roadmap for the relevant organisation in addressing gaps identified after the audit; accordingly, this approach indicates that this study is a gap analysis that examines all other sources and how the right implementations should be made by making use of them.

Before explaining the basic features and formulation of the Persona-based assessment kit, it should be stated that; the number of personas within the organisation and the responses each persona give to the questions were specific to that particular organisation. Additionally, only some persons are obliged to answer every question due to the specific nature of their role within the organisation or their level of access and responsibilities within the organisation’s technical infrastructure. The number and type of questions each persona is asked to respond to are determined based on their specific role and responsibilities within the organisation and their level of access and influence on the security of the technical infrastructure. This is done to ensure that the analysis accurately reflects the level of risk and trust placed on each persona within the organisation and to obtain a comprehensive and accurate assessment of the organisation’s overall persona-based resiliency score.

Accordingly, the Zero-Trust value for each persona was also unique to the organisation. By combining these values, the resiliency score for the organisation was obtained through the calculation of a weighted average between 0 and 100.

The objective of this analysis is to determine the resiliency level of the organisation by considering the number of personas, the responses given by each persona, and the respective Zero-trust Values. By analysing these values, the study aims to understand the organisation’s cybersecurity posture in the name of resiliency and highlight areas for improvement.

When calculating the organisation's overall cyber resiliency score, only 30% of this assessment's score is included due to the question content and amount of the persona-based assessment.

The values required to calculate the persona-based cyber resiliency are Number of Persona, Number of Audit Questions, the Value of Zero-trust, the Number of "Yes" Answers and finally Persona-Based Score.

An example of a Persona-based assessment kit can be observed in Appendix C.

3.6.1 Number of Persona (np)

This value represents the number of persons in the organisation which held the assessment. This value is expressed as "np" in the main formula.

3.6.2 Number of Audit Questions (naq)

In the main formulation, this value is expressed as "naq". The number of audit questions refers to the number of questions to be answered by a relevant persona.

3.6.3 Value of Zero-trust (VZT)

In the main formulation, this value is expressed as "VZT". It represents the Zero-Trust value of the relevant persona in the organisation, ranges from 0 to 100, and is used to determine weight when taking the weighted average. This value is determined by the relevant organisation's CTO, IT Director or CISO. This value prioritises protecting sensitive data and systems by assuming that all actors are potentially malicious until they have been proven otherwise through proper authentication and authorisation processes. It also reflects the risk appetite of the persona in the relevant organisation.

3.6.4 Number of “Yes” Answers (nya)

In the main formulation, this value is expressed as “nya”. It refers to the number of questions that were answered as “Yes” (meaning of; “for the related persona, the security control mentioned in the related ability control question is operated.”) for the relevant persona.

3.6.5 Persona-Based Score (PBS)

In the main formulation, this value is expressed as “PBS”. For the related persona, the value shows the extent to which the related ability control questions are operated. It represents the score of each persona out of 100.

$$PBS = \frac{nya \cdot 100}{naq} \quad (3.6.5.a)$$

3.6.6 Calculation of the Score of Persona-Based Assessment Result (PB)

To calculate the weighted average, i.e., the score that gives the organisation’s resilience from the Persona-Based Zero-trust perspective, add the product of the personas’ *VZT* and *PBS* up to the Number of Persona and divide by the sum of the personas’ *VZT*.

$$PB = \frac{\sum_{k=1}^{np} PBS_k \cdot VZT_k}{\sum_{k=1}^{np} VZT_k} \quad (3.6.6.a)$$

The result of this calculation provides valuable insights into the organisation’s ability to protect sensitive data and systems from potential security threats. It helps make informed decisions to improve the organisation’s overall security posture.

3.7 Total Cyber Resiliency Score Of the Organization

It is calculated based on the scores of persona-based and risk-based assessments.

$$\text{Total Cyber Resiliency Score} = PB \cdot 0,3 + RB \cdot 0,7 \quad (3.7.a)$$

4. RESULTS AND ANALYSIS

4.1 Case Studies: Application of the Cyber Resiliency Ability Control Assessments

Organizations in different sizes and sectors participated in this research. Due to the differences in sizes for each organization, an audit was carried out with assessment kits prepared with appropriate questions. For example, the audit kits used for large-sized organization and small-sized organization are not the same; IT infrastructure components audited for large-sized organization are not suitable for small-sized organization.

4.1.1 Overview of the Assessed Organizations

This chapter provides an overview of the organisations evaluated during this research investigation. Five organisations, whose size and structure varied significantly, participated in this study. These include a large-scale organisation, a medium-sized organisation, a small and medium-sized enterprise (SME), and a university.

In order to maintain confidentiality and adhere to the principles of ethical research, the specific identities and industries of these organisations will not be disclosed. However, certain distinguishing characteristics will be highlighted to illustrate their differences. These characteristics include the total number of employees, the diversity and number of departments within each organisation, specific information regarding the structure of their IT departments, and their respective cyber resiliency scores.

By highlighting these distinctions, this section aims to provide a nuanced comprehension of each organisation's unique context, thereby elucidating how these factors may influence the cyber resilience outcomes of each organisation. The adaptive nature of the proposed risk-based cyber resiliency ability control kit and the persona-based zero-trust cyber resiliency ability control kit can be understood through these distinctions. In turn, this demonstrates the adaptability and scalability of these tools when applied in various organisational contexts.

4.1.1.1 Large-sized organisation

The following assessment pertains to a large-scale organisation, which will not be identified by name in the interest of anonymity. However, it is important to note that this organisation is renowned and widely recognised globally within its respective industry. It lies on the lower end of the risk spectrum, a sector other than high-risk industries such as finance or healthcare.

This organisation boasts a substantial workforce, numbering approximately 110,000 employees. Its organisational structure comprises nine primary departments, each further branching into various functional units, indicating a highly differentiated and potentially complex internal environment.

The IT department within this organisation presents a relatively modern infrastructure, segmented into eight distinct functions, although legacy systems remain, particularly within their server technology. Such an environment can present unique challenges and opportunities regarding cyber resiliency.

Upon conducting the Risk-Based audit, the organisation scored 87.97, demonstrating high resilience. Conversely, in the Persona-based audit, the organisation scored slightly lower, at 78.29. When averaged, the organisation has an overall cyber resiliency score of 85.02.

Analysing this score, the organisation exhibits a relatively robust cybersecurity posture. Despite being in a low-risk industry, the organisation has taken significant steps towards implementing solid cybersecurity controls, as indicated by its high Risk-Based audit score. However, the lower Persona-Based audit score suggests room for improvement in tailoring their cybersecurity practices to the unique risks faced by different personas or roles within the organisation.

Given the large size and complexity of the organisation, maintaining such a high overall cyber resiliency score is commendable. However, continuous improvement should be

sought to address identified weaknesses and ensure ongoing resilience in the face of ever-evolving cyber threats.

With the organisation's consent, the audit report created for it may be displayed in this thesis. Readers can see this organisation's audit report in Appendix D.

4.1.1.2 Medium-sized organisation

The subsequent evaluation pertains to a medium-sized organisation operating in a high-risk industry. This non-financial industry involves managing sensitive information about individuals and organisations, necessitating stringent security measures. To maintain confidentiality, neither the organisation's name nor its industry will be disclosed.

This organisation has approximately 280 employees, which is a relatively modest number. Its organisational structure is relatively straightforward, with only two of its five primary departments subdivided into distinct functional divisions. Its IT department is divided into three distinct functions and relies predominantly on modern infrastructure, which may increase its resilience against cyber threats.

The organisation's risk-based audit score is 91.73, and its persona-based audit score is even higher at 95.38, resulting in an average cyber resiliency score of 92.82. This analysis indicates that the organisation has a commendable level of cyber resilience.

The organisation has effectively implemented robust cybersecurity controls despite operating in a high-risk industry, as evidenced by its high scores in both risk-based and persona-based audits. The high persona-based audit score is particularly noteworthy, indicating that the organisation has effectively tailored its cybersecurity practices to mitigate the specific risks associated with various roles.

Given the nature of the information handled by the organisation, a robust cybersecurity posture is essential. The consistently high scores across both audits indicate a well-integrated and comprehensive approach to cybersecurity, which is commendable given the organisation's scale and the industry's high-risk nature. The organisation is current.

Additionally, IT infrastructure contributes positively to its resilience score, enhancing its capacity to defend against modern cyber threats.

Its organisational structure's relative simplicity may also contribute to its capacity to implement and maintain robust security controls. This medium-sized organisation exemplifies a commitment to cyber resilience that is exemplary. Nevertheless, given the sensitive nature of the data it manages and the dynamic nature of cyber threats, it should endeavour to maintain and continuously enhance its robust cybersecurity posture.

4.1.1.3 SME

The analysis concentrates on a small or medium-sized business (SME) operating in a low-risk industry. As a consulting firm, despite the low-risk character of this industry, this business maintains sensitive client information. To maintain anonymity, the specifics of the organisation and industry are concealed.

The small- to medium-sized business has a streamlined structure with about 40 employees. Only two of its four main departments are subdivided into specific functions. This organisational structure proposes a straightforward, streamlined approach to operations management. This organisation's IT department is straightforward, consisting predominantly of on-site support. Modern IT infrastructure can potentially increase the SME's cyber resilience.

The organisation's cyber resilience was evaluated using risk-based and persona-based audits, yielding 72.98 and 64.24, respectively. This resulted in a score of 70.35 overall.

Inferring from these results, the SME has achieved a moderate level of cyber resilience. The slightly above-average risk-based audit score indicates satisfactory alignment with standard cybersecurity controls. Even though the persona-based audit score is lower, it indicates that there has been some success in tailoring cybersecurity practices to specific organisational positions. However, there is still room for improvement.

The SME is a consulting firm that handles vital client data, so its cyber resilience should be exceptionally high. Despite its scale, the SME must take stringent precautions to ensure client data's confidentiality, integrity, and availability, which are essential for maintaining trust and business continuity.

The organisation has a modern IT infrastructure and a streamlined organisational structure. However, there is room for development, particularly in implementing more personalised, role-based security measures. Expansion of the IT department to include more specialised functions could be a development area.

While the SME has made significant efforts to create a cyber-resilient environment, additional strategic, role-specific, and comprehensive cybersecurity measures are required to improve their resilience score and, more importantly, their security posture.

4.1.1.4 Small-sized organisation

The entity under scrutiny in this instance is an enterprise of a modest scale, functioning as a nascent start-up in the internet media sector, which is typically identified as carrying a low degree of risk. The organisation's specific particulars have been intentionally obscured to safeguard anonymity.

Consisting of a small team of 5 to 8 individuals, this start-up is characterised by a non-hierarchical structure, lacking the conventional compartmentalisation into distinct departments. Instead, it exhibits a unified team dynamic that tackles the vast majority of the required tasks. Specialist operations, such as financial management and IT support, are not handled internally but outsourced to external consultants, demonstrating the start-up's nimbleness and adaptability.

Notably, the absence of a dedicated IT department suggests a reliance on external support for information technology concerns, potentially creating a gap in comprehensive, ongoing supervision of their IT infrastructure and cybersecurity controls.

The start-up's resilience to cyber threats was evaluated via two distinct audits: a Risk-Based audit and a Persona-Based audit. These assessments yielded scores of 69.23 and 11.48, respectively, culminating in a combined score of 51.91.

Despite its small scale and absence of an in-house IT department, the organisation's Risk-Based audit score shows a considerable implementation of conventional cybersecurity controls, indicating satisfactory resilience to cyber threats. However, the Persona-Based audit score, being significantly lower, reveals a substantial deficit in adapting cybersecurity practices to the unique roles within the organisation, an essential aspect of maintaining a robust cybersecurity stance.

In summation, while the small-sized start-up presents a moderate level of resilience to cyber threats, the substantial potential exists for improvement, particularly in role-specific cybersecurity practices. This organisation should strive to comprehend that the goal of strong cyber resilience extends beyond simple risk mitigation, including fostering trust, driving innovation, and facilitating growth.

4.1.1.5 University

The institution in question is a university, which presents special difficulties and complexities because of the wide range of stakeholders involved, including staff, students, and outside organisations. The assessed university has a lot of sensitive information that needs to be secured, including intellectual property and the personal information of staff and students, despite not being in a typically high-risk sector. The university has a staff of about 400 people and is organised into ten different departments, reflecting the wide range of academic specialities and functional areas in such an organisation.

The assessed university is assessed on the same level as a large organisation due to its enormous size and complexity in terms of staff numbers and the multifaceted nature of its operations. Notably, the university's IT department consists of six distinct functional divisions, which is evidence of the importance of digital infrastructure in the contemporary educational environment. However, the efficiency of this department's

operation depends not only on its size but also on how well it complements the various operational facets of the university.

This university received scores of 50.34 and 25.64 from the dual audits of the risk-based and persona-based evaluations for a final score 42.92. This finding demonstrates a significant gap between the university's risk-based and persona-based audit scores, demonstrating that while some basic information security measures have been implemented, more role-specific cybersecurity practices and measures should be needed. This shortcoming may be attributed to a university's complex and diverse nature, where it can be difficult to implement personalised and role-specific cybersecurity practices across various departments and roles.

However, given the sensitivity of the data handled and the potential repercussions of a cybersecurity breach within an educational institution, the relatively low persona-based score indicates an area urgently needing improvement.

In conclusion, the university needs to exhibit more role-specific cybersecurity practices, despite displaying moderate resilience to cyber threats overall. This discrepancy highlights the urgent need to strengthen cybersecurity measures and ensure they align with the particular difficulties brought on by the various roles and functions within the educational sector.

With the assessed university's consent, the audit report created for it is displayed in this thesis. Readers can see this organisation's audit report in Appendix D.

5. DISCUSSION

5.1 Summary of the Main Findings

This study aims to evaluate and demonstrate the cyber resiliency of organisations of different sizes, namely a large-sized organisation, a medium-sized organisation, a small and medium-sized enterprise (SME), a small-sized organisation, and a university, employing both Risk-Based and Persona-Based assessment kits. The assessment scores from these audits provided an insightful and nuanced understanding of the organisation's cybersecurity postures.

As a globally renowned brand, the large-sized organisation demonstrated a commendable overall resilience score of 85.02, indicating robust cybersecurity measures. While the Risk-Based score was slightly higher than the Persona-Based score, the disparity was insignificant, signifying a balanced approach to general and role-specific cyber resilience measures. Nonetheless, room for further refinement exists, particularly in enhancing persona-based cybersecurity practices.

Despite operating in a high-risk sector, the medium-sized organisation achieved the highest resilience score of 92.82. It demonstrated a noteworthy Persona-Based score of 95.38, indicating a strong alignment of cybersecurity measures with specific organisational roles and responsibilities. The high scores reflect the organisation's committed effort in securing sensitive data about individuals and other organisations, given the high-risk nature of its operations.

The SME, a consulting firm with sensitive client data, displayed a good cyber resilience score of 70.35. However, the noticeable difference between its Risk-Based and Persona-Based scores suggested an area for improvement, particularly in implementing role-specific security measures.

The small-sized organisation, an internet media startup, recorded the lowest resilience score of 51.91. While it had an average Risk-Based score, its Persona-Based score was

drastically lower, suggesting significant deficiencies in its role-specific cybersecurity practices. As a startup, this underscores the necessity to prioritise cybersecurity from its nascent stages.

Even with its status as a significant educational institution with a multitude of stakeholders, it displayed the lowest cyber resilience score of 42.92. The stark discrepancy between its Risk-Based and Persona-Based scores underscored the challenges in implementing effective, role-specific cybersecurity measures in a complex educational environment.

These findings underscore the criticality of comprehensive and role-specific cybersecurity measures in organisations of all sizes and sectors. They also highlight the need to align cyber resilience strategies with the organisation's specific operational context and risk profile.

5.2 Implications Of The Research For Organizations And Cybersecurity Practitioners

This study has significant ramifications for organisations across the spectrum of size and structure and for cybersecurity professionals tasked with ensuring information security. It demonstrates that the level of cyber resilience within an organisation is not necessarily proportional to its size. Rather, it focuses on the significance of strategic, context-aware, and persona-specific cybersecurity practices in fostering a robust cyber resilience profile.

The findings provide cybersecurity professionals with a nuanced understanding of the effectiveness of a dual-audit approach. This strategy integrates risk-based and persona-based cybersecurity resilience measures, making it a valuable addition to their cybersecurity arsenal. The disparity in audit scores between various organisations highlights the need for an all-encompassing, well-rounded, and multifaceted cybersecurity strategy. Such a strategy necessitates combining standard information security measures with those tailored to specific organisational roles or personas.

Importantly, the findings call for a paradigm shift in the conception of cybersecurity strategies. No longer is it sufficient to apply a uniform, unidimensional strategy to all entities. This study emphasises the potential for any organisation, regardless of size or industry, to achieve high levels of cyber resilience. This objective becomes attainable when organisations have an in-depth understanding of their unique operational context. In addition, a commitment must be made to deploying generic and mission-specific cybersecurity measures.

The research, in its entirety, highlights the shift towards a more tailored, dynamic, and context-sensitive approach to cybersecurity. This strategy enables organisations to navigate the complex landscape of cyber threats more effectively, enhancing their resilience against potential cyberattacks.

5.3 Limitations Of The Study And Potential Areas For Future Research

By definition, every empirical study has inherent limitations, and this investigation is not exempt from such limitations. First, the analysis was based on a small sample size of five organisations, which may not represent the wide range of organisational sizes, industries, and complexities. This factor might affect the generalizability of the results.

In addition, the study minimises the dynamic nature of cybersecurity. Cyber threats and vulnerabilities constantly evolve; any assessment is a snapshot of an organisation's cybersecurity resilience at any particular time. Future research should take a longitudinal approach to measure changes in the cybersecurity resilience of an organisation over time.

In terms of future research, several areas have potential for investigation. Advanced data analytics or machine learning techniques could be used to identify cyber resilience patterns or predictors. This could provide organisations with valuable insights for designing their cybersecurity strategies.

In addition, future research could investigate the influence of organisational factors such as organisations' culture and leadership style on cyber resilience. Developing industry-

specific audit methodologies to account for different industries' unique cybersecurity challenges is a potential avenue for future research.

One of the thesis' limitations is the weighting ratio used in calculating the total cyber resiliency score, which is 70 points for the risk-based assessment and 30 points for the persona-based assessment. The chosen ratio was created with the goal of reflecting the perceived relative importance of risk-based factors versus persona-based factors within the context of the organisations under consideration. In this study, the risk-based assessment encompasses a broader spectrum of potential threats and vulnerabilities that may affect an organization's cybersecurity posture, hence the higher weightage. In contrast, the persona-based assessment, which accounts for 30 points, focuses on more specialised and context-sensitive aspects of cyber resilience.

It is acknowledged, however, that this ratio may not be universally applicable across various organisational contexts and industries. The decision to use this specific weighting was made after conducting a literature review, consulting with experts, and considering the unique characteristics of the participating organisations. Nonetheless, future research could look into different weighting mechanisms, and more empirical evidence may be needed to validate or modify this ratio. Although the chosen ratio was deemed appropriate for the scope of this study, it remains a potential limitation that future scholars in the field may wish to investigate further.

By openly admitting this limitation, the thesis reaffirms its commitment to academic rigour and transparency while also highlighting an area that may benefit from additional investigation and methodological refinement in future research.

The design of the assessment kits used in this study may also be important to note. Particularly, the potential use of a Likert scale in place of the current methodology's binary "yes/no" framework for collecting responses.

The binary method applied in this study provided a clear and succinct way to assess how well-aligned a company is with various cyber resilience factors. The granularity and

nuance with which some aspects of cyber resilience can be explored, though, may be constrained by this simplicity.

A Likert scale, which typically offers a range of responses from "strongly disagree" to "strongly agree," could be included to allow respondents to express different levels of agreement or certainty. This method may be able to capture more subtle variations in how different organisations perceive and apply cyber resilience measures.

While the desire for clarity and consistency across different organisations and assessments served as the driving force behind the choice to use a binary response mechanism, it is acknowledged that a Likert scale might provide richer data and allow for more in-depth analyses. The proposed use of a Likert scale opens up an intriguing area for future study and suggests a potential methodological improvement that might deepen and fine-tune assessments of cyber resilience.

This restriction draws attention to a decision made in the study design that future researchers may want to revisit without necessarily reducing the validity of the research findings in the context. The choice between a binary and a Likert scale would ultimately depend on the particular research questions, objectives, and contexts being addressed, and the inclusion of a Likert scale presents an exciting opportunity for further investigation in the area of cyber resilience.

In conclusion, while this study provides valuable insights into the evaluation of cyber resilience, it is mostly a foundational work toward a much-needed expansion and deepening of research in this vital field.

6. CONCLUSION

The purpose of the study was to investigate and analyse the concept of cyber resilience within organisations of various sizes. Developing and applying an innovative 'Risk-Based Cyber Resiliency Assessment Kit' was a key tool in accomplishing this. This tool's main strength is its comprehensive, dual-pronged auditing approach, including risk-based and persona-based evaluations. This multi-dimensional methodology was meticulously designed to adapt to each organisation's unique characteristics and specificities, effectively considering the organisation's size and distinct security needs.

The assessment kit was thoroughly explained, outlining its key features and dynamic structure. The modularity of the kit enables it to cater to a wide range of organisations, from large corporations to small start-ups, each with its own set of information security requirements. Furthermore, the fundamental components of information security - Confidentiality, Integrity, and Availability (CIA) - were used as assessment underpinning principles. Combined with a different scoring system based on Likelihood or Effectiveness (LE), these measures resulted in a sophisticated and nuanced standardising formula. For each control question, this formula produced a Control's Risk Score (CRS) out of five, a scoring strategy that provides a granular understanding of the organisation's security standing.

The methodology, as described, was meticulously applied to a diverse group of five organisations, each of which differed in size and sector. The participating organisations ranged from large multinational corporations to small start-ups, including a medium-sized organisation, an SME, and a university. These organisations' commitment to maintaining their anonymity was unwavering throughout the process, with all assessments conducted confidentially and ethically. Each organisation's distinct characteristics, such as its IT structure and employee count, were thoroughly examined.

Due to these comprehensive audits, we obtained a risk-based audit score and a persona-based audit score for each organisation. This dual-scoring system provided us with a comprehensive and precise understanding of the various levels of cyber resilience present

in the participating organisations. These findings revealed that an organisation's cyber resilience cannot be attributed solely to size. Instead, it became clear that a strategic, comprehensive, and context-sensitive approach to cybersecurity measures contributes significantly to increased resilience.

The study advocated for a more tailored and dynamic methodology, recognising the need to move beyond a traditional, one-dimensional approach to cybersecurity. This approach integrates an organisation's unique operational context with generic and mission-specific cybersecurity measures, resulting in a more context-sensitive and adaptive cyber threat defence strategy.

We also acknowledged the study's limitations, which included sample size, audit nature, reliance on self-reported data, and the fluid and evolving nature of cybersecurity threats. Despite these constraints, the limitations revealed potential avenues for future research, emphasising the importance of investigating advanced data analytics and machine learning in cybersecurity, understanding the impact of organisational factors on cyber resilience, and developing industry-specific audit methodologies.

To summarise, this thesis thoroughly examines cyber resilience, shedding light on its multifaceted nature and the need for a nuanced, context-specific approach to assessing and improving it. The findings highlight the importance of strategic and context-aware cybersecurity practices, providing valuable insights for organisations of all sizes and sectors.

BIBLIOGRAPHY

- Ahmad, Maqsood, Syed Zulfiqar Ali Shah, and Yasar Abbass. 2020. "The Role of Heuristic-Driven Biases in Entrepreneurial Strategic Decision-Making: Evidence from an Emerging Economy." *Management Decision* 59 (3): 669–91. <https://doi.org/10.1108/MD-09-2019-1231/FULL/PDF>.
- Ahmadi-Assalemi, Gabriela, Haider Al-Khateeb, Gregory Epiphaniou, and Carsten Maple. n.d. "Cyber Resilience and Incident Response in Smart Cities: A Systematic Literature Review." Accessed May 3, 2023. <https://doi.org/10.3390/smartcities3030046>.
- Alotaibi, Mutlaq, Steven Furnell, and Nathan Clarke. 2017. "Information Security Policies: A Review of Challenges and Influencing Factors." In *2016 11th International Conference for Internet Technology and Secured Transactions, ICITST 2016*, 352–58. Institute of Electrical and Electronics Engineers Inc. <https://doi.org/10.1109/ICITST.2016.7856729>.
- Amankwah-Amoah, Joseph, Zaheer Khan, Geoffrey Wood, and Gary Knight. 2021. "COVID-19 and Digitalization: The Great Acceleration." *Journal of Business Research* 136 (November): 602–11. <https://doi.org/10.1016/J.JBUSRES.2021.08.011>.
- Basta, Nardine, Muhammad Ikram, Mohamed Ali Kaafar, and Andy Walker. 2022. "Towards a Zero-Trust Micro-Segmentation Network Security Strategy: An Evaluation Framework." *Proceedings of the IEEE/IFIP Network Operations and Management Symposium 2022: Network and Service Management in the Era of Cloudification, Softwarization and Artificial Intelligence, NOMS 2022*. <https://doi.org/10.1109/NOMS54207.2022.9789888>.
- Bauer, Stefan, Edward W.N. Bernroider, and Katharina Chudzikowski. 2017. "Prevention Is Better than Cure! Designing Information Security Awareness Programs to Overcome Users' Non-Compliance with Information Security Policies in Banks." *Computers & Security* 68 (July): 145–59. <https://doi.org/10.1016/J.COSE.2017.04.009>.
- Berners-Lee, Tim. 2010. "Long Live The Web" 303 (6): 80–85. <https://doi.org/10.2307/26002308>.
- Bodeau, Deborah, Richard Graubart, and M A Bedford. 2017. "Cyber Resiliency Design Principles: Selective Use Throughout the Lifecycle and in Conjunction with Related Disciplines."
- Chopra, Abhishek, and Mukund Chaudhary. 2020. "Implementing an Information Security Management System." *Implementing an Information Security Management System*. <https://doi.org/10.1007/978-1-4842-5413-4>.

- Connolly, Lena Yuryna, David S Wall, Michael Lang, and Bruce Oddson. n.d. "An Empirical Study of Ransomware Attacks on Organizations: An Assessment of Severity and Salient Factors Affecting Vulnerability." Accessed May 3, 2023. <https://doi.org/10.1093/cybsec/tyaa023>.
- Constantinides, Panos, Ola Henfridsson, and Geoffrey G Parker. 2018. "Introduction-Platforms and Infrastructures in the Digital Age." *Information Systems Research* 29 (2): 381–400. <https://doi.org/10.1287/isre.2018.0794>.
- Curran, James, Natalie Fenton, and Des Freedman. 2012. "Rethinking Internet History: James Curran." *Misunderstanding the Internet*, March, 40–71. <https://doi.org/10.4324/9780203146484-6>.
- Danquah, Paul, Stephen Bekoe, and Victor Gordon. 2022. "An Empirical Assessment of Information Security Best Practices and Information Technology Disaster Recovery Readiness in Ghanaian Micro-Finance Sector." *International Journal of Business Continuity and Risk Management* 12 (1): 42–61. <https://doi.org/10.1504/IJBCRM.2022.121647>.
- Fikri, Ahmad Maulana, Lovinta Happy Atrinawati, and Muhammad Gilvy Langgawan Putra. 2022. "Cyber Resilience Evaluation Using Cyber Resilience Review Framework at University XYZ." *International Journal of Educational Management and Innovation* 3 (2): 155–68. <https://doi.org/10.12928/IJEMI.V3I2.5794>.
- Furnell, S. M., P.S. Dowland, and P.W. Sanders. 1999. "Dissecting the Hacker Manifesto." *Information Management & Computer Security* Vol. 7 (No. 2): 69–75. <https://www.emerald.com/insight/content/doi/10.1108/09685229910265493/full/html>.
- Furnell, Steven. 2021. "The Cybersecurity Workforce and Skills." *Computers and Security* 100 (January). <https://doi.org/10.1016/J.COSE.2020.102080>.
- Ignat, Inga. 2022. "Factor Analysis of Information Risk (FAIR™) When Assessing the Information Security." Moldova: Institutional Repository of the Technical University of Moldova.
- Kaushik, Neeraj, and Teena Bagga. 2020. "Internet of Things (IoT): Implications in Society." In *SSRN Electronic Journal*. Elsevier BV. <https://doi.org/10.2139/SSRN.3563104>.
- Kergel, David. 2019. *The History of the Internet: Between Utopian Resistance and Neoliberal Government*. Edited by Peter Pericles Trifonas. Switzerland: Springer, Cham. https://doi.org/10.1007/978-3-319-56988-8_13.
- Kleij, Rick van der, and Rutger Leukfeldt. 2020. "Cyber Resilient Behavior: Integrating Human Behavioral Models and Resilience Engineering Capabilities into Cyber Security." *Advances in Intelligent Systems and Computing* 960: 16–27. https://doi.org/10.1007/978-3-030-20488-4_2/COVER.

- Klein, Dave. 2021. "Micro-Segmentation: Securing Complex Cloud Environments." *https://doi.org/10.1016/S1353-4858(19)30034-0* 2019 (3): 6–10. [https://doi.org/10.1016/S1353-4858\(19\)30034-0](https://doi.org/10.1016/S1353-4858(19)30034-0).
- Krumay, Barbara, Edward W.N. Bernroider, and Roman Walser. 2018. "Evaluation of Cybersecurity Management Controls and Metrics of Critical Infrastructures: A Literature Review Considering the NIST Cybersecurity Framework." *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 11252 LNCS: 369–84. https://doi.org/10.1007/978-3-030-03638-6_23/TABLES/4.
- Lallie, Harjinder Singh, Lynsay A. Shepherd, Jason R.C. Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens. 2021. "Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic." *Computers & Security* 105 (June): 102248. <https://doi.org/10.1016/J.COSE.2021.102248>.
- Lykou, Georgia, Argiro Anagnostopoulou, and Dimitris Gritzalis. 2018. "Implementing Cyber-Security Measures in Airports to Improve Cyber-Resilience." *2018 Global Internet of Things Summit, GIoTTS 2018*, November. <https://doi.org/10.1109/GIOTS.2018.8534523>.
- Mailloux, Logan O., Paul M. Beach, and Martin Trae Span. 2018. "Examination of Security Design Principles from NIST SP 800-160." *12th Annual IEEE International Systems Conference, SysCon 2018 - Proceedings*, May, 1–8. <https://doi.org/10.1109/SYSCON.2018.8369491>.
- Mailloux, Logan O., and Michael Grimaila. 2018. "Advancing Cybersecurity: The Growing Need for a Cyber-Resiliency Workforce." *IT Professional* 20 (3): 23–30. <https://doi.org/10.1109/MITP.2018.032501745>.
- Malatji, Masike, Annlizé L Marnewick, and Suné Von Solms. 2022. "Cybersecurity Capabilities for Critical Infrastructure Resilience Cybersecurity Capabilities 255." *Information & Computer Security* 30 (2): 255–79. <https://doi.org/10.1108/ICS-06-2021-0091>.
- Margherita, Alessandro, and Marikka Heikkilä. 2021. "Business Continuity in the COVID-19 Emergency: A Framework of Actions Undertaken by World-Leading Companies." *Business Horizons* 64 (5): 683–95. <https://doi.org/10.1016/J.BUSHOR.2021.02.020>.
- Mazzolin, Robert, and Asad Madni. 2020. "A Survey of Contemporary Cyber Security Vulnerabilities and Potential Approaches to Automated Defence." *SYSCON 2020 - 14th Annual IEEE International Systems Conference, Proceedings*, August. <https://doi.org/10.1109/SYSCON47679.2020.9275828>.

- Meriah, Ines, and Latifa Ben Arfa Rabai. 2019. "Comparative Study of Ontologies Based ISO 27000 Series Security Standards." *Procedia Computer Science* 160 (January): 85–92. <https://doi.org/10.1016/J.PROCS.2019.09.447>.
- Möller, Dietmar P.F. 2023. "NIST Cybersecurity Framework and MITRE Cybersecurity Criteria." *Advances in Information Security* 103: 231–71. https://doi.org/10.1007/978-3-031-26845-8_5/COVER.
- Nambisan, Satish, Mike Wright, and Maryann Feldman. 2019. "The Digital Transformation of Innovation and Entrepreneurship: Progress, Challenges and Key Themes." *Research Policy* 48 (8): 103773. <https://doi.org/10.1016/J.RESPOL.2019.03.018>.
- Packard, Noel. 2020. "The ARPANET Into the Internet: A Tale of Two Networks." *Studies in Media and Communication* 8 (1). <https://doi.org/10.11114/smc.v8i1.4783>.
- Pillitteri, Victoria, Ehijele Olumese, Esten Porter, David Black, Eduardo Takamura, McKay Tolboe, Lydia Humphries, et al. 2020. "NIST Special Publication 800-53 Revision 5 Security and Privacy Controls for Information Systems and Organizations." <https://doi.org/10.6028/NIST.SP.800-53r5>.
- Prabhu Kavin, Balasubramanian, Sannasi Ganapathy, U. Kanimozhi, and Arputharaj Kannan. 2020. "An Enhanced Security Framework for Secured Data Storage and Communications in Cloud Using ECC, Access Control and LDSA." *Wireless Personal Communications* 115 (2): 1107–35. <https://doi.org/10.1007/s11277-020-07613-7>.
- Rose, Scott, Oliver Borchert, Stu Mitchell, and Sean Connelly. 2020. "Zero Trust Architecture," August. <https://doi.org/10.6028/NIST.SP.800-207>.
- Ross, Ron, Victoria Pillitteri, Richard Graubart, Deborah Bodeau, and Rosalie Mcquaid. 2021. "NIST Special Publication 800-160, Volume 2 Developing Cyber-Resilient Systems: A Systems Security Engineering Approach." <https://doi.org/10.6028/NIST.SP.800-160v2r1>.
- Roy, Prameet P. 2020. "A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard." *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications, NCETSTEA 2020*, February. <https://doi.org/10.1109/NCETSTEA48365.2020.9119914>.
- Ryan, Johnny. 2010. *A History of the Internet and the Digital Future*. 33 Great Sutton St. London United Kingdom: Reaktion Books. https://books.google.com.tr/books?hl=tr&lr=&id=l0OYhHefumoC&oi=fnd&pg=PP1&dq=johnny+ryan+a+history+of+the+internet+and+the+digital+future&ots=GTk1XdMD2W&sig=oitE7ycHaAEMwZDPRMjil0uHQyM&redir_esc=y#v=onepage&q=johnny%20ryan%20a%20history%20of%20the%20internet%20and%20the%20digital%20future&f=false.

- Sharma, Dr N K, and Prabir Kumar Dash. 2012. "Effectiveness Of Iso 27001, As An Information Security Management System: An Analytical Study Of Financial Aspects." *Far East Journal of Psychology and Business*, no. 5: 57–71. <https://ideas.repec.org/a/fej/article/v9cy2012i5p57-71.html>.
- Shore, Malcolm, Sherali Zeadally, and Astha Keshariya. 2021. "Zero Trust: The What, How, Why, and When." *Computer* 54 (11): 26–35. <https://doi.org/10.1109/MC.2021.3090018>.
- Simpson, William R, and Kevin E Foltz. n.d. "Network Segmentation and Zero Trust Architectures." Accessed May 7, 2023.
- Singh, Sonika, and Joffre Swait. 2017. "Channels for Search and Purchase: Does Mobile Internet Matter?" *Journal of Retailing and Consumer Services* 39 (November): 123–34. <https://doi.org/10.1016/J.JRETCONSER.2017.05.014>.
- Targowski, Andrew. 2005. "From the Cold War to Internet Cathedral." *International Journal of Information and Communication Technology Education* 1 (2): 87–99. <https://doi.org/10.4018/JICTE.2005040108>.
- Teerakanok, Songpon, Tetsutaro Uehara, Atsuo Inomata, and Qi Li. 2021. "Migrating to Zero Trust Architecture: Reviews and Challenges." <https://doi.org/10.1155/2021/9947347>.
- Turnbull, Benjamin. 2018. "Cyber-Resilient Supply Chains: Mission Assurance in the Future Operating Environment." *Australian Army Journal Cyber-Warfare Edition* XIV (3). <https://doi.org/10.3316/IELAPA.344417545553155>.
- Urbach, Nils, and Maximilian Röglinger. 2019. "Introduction to Digitalization Cases: How Organizations Rethink Their Business for the Digital Age," 1–12. https://doi.org/10.1007/978-3-319-95273-4_1.
- Vetter, Ronald J., Chris Spell, and Charles Ward. 1994. "Mosaic and the World-Wide Web." *Computer* 27 (10): 49–57. <https://doi.org/10.1109/2.318591>.
- Volkodaeva, A. V., A. V. Balanovskaya, and E. A. Rustenova. 2022. "Trends in Information and Communication Technologies Development in Context of Economy Digitalization." *Lecture Notes in Networks and Systems* 304: 583–92. https://doi.org/10.1007/978-3-030-83175-2_72/COVER.
- Wagner, Neal, Cem S. Sahin, Michael Winterrose, James Riordan, Jaime Pena, Diana Hanson, and William W. Streilein. 2017. "Towards Automated Cyber Decision Support: A Case Study on Network Segmentation for Security." *2016 IEEE Symposium Series on Computational Intelligence, SSCI 2016*, February. <https://doi.org/10.1109/SSCI.2016.7849908>.
- Zeijlemaker, Sander, Etiënne A.J.A. Rouwette, Giovanni Cunico, Stefano Armenia, and Michael von Kutzschenbach. 2022. "Decision-Makers' Understanding of Cyber-

Security's Systemic and Dynamic Complexity: Insights from a Board Game for Bank Managers.” *Systems* 2022, Vol. 10, Page 49 10 (2): 49. <https://doi.org/10.3390/SYSTEMS10020049>.



APPENDIX A

A.1 Sample of Voluntary Participation Consent Form

Voluntary Participation Consent Form
Title of the Study: Cyber Resilience Ability Control Assessment On A Risk Centric And Persona Based Ztna Approach
Researcher: Yaprak Kurtlutepe
Purpose of the Study: This study aims to assess the applicability of the cyber resiliency assessment kit developed as part of a master's thesis. Your organisation's participation will help validate the effectiveness and usefulness of this assessment kit for organisations of various sizes and sectors. The research involves collecting basic measurements related to cybersecurity, and no identifying information about individual participants or the organisation will be obtained. Procedures: If your organisation agrees to participate in this study, you will be asked to: 1. The researcher can conduct a cyber resilience assessment using two different assessment kits. 2. Provide access to relevant information, systems, and personnel required for the assessment. 3. Participate in follow-up discussions or interviews about the assessment findings and recommendations.
Voluntary Participation: Your organisation's participation in this study is entirely voluntary. Your organisation can withdraw from the study without penalty or loss of benefits. If your organisation decides to withdraw, all information collected up to that point will be destroyed.
Confidentiality and Anonymisation: All information collected during this study will be kept strictly confidential and anonymised to ensure that no individual or organisational identifiers are present in the data. No personally identifiable information or specific organisational details will be shared or published. Data collected will be stored securely, and only the researcher and authorised personnel will have access to it. Upon completion of the study, all data collected will be destroyed securely.
Risks and Benefits: There are minimal risks associated with participating in this study. The cybersecurity risk assessment process is non-invasive, and the researcher will take all necessary precautions to minimise disruptions to your organisation's daily operations. The potential benefits of participating in this study include gaining valuable insights into your organisation's cybersecurity posture and receiving recommendations for improving your security measures.
Questions: If you have any questions or concerns about this study or your organisation's participation, please contact the researcher at [yaprakurtlutepe@gmail.com].
Consent: By signing this form, you acknowledge that you understand the purpose of the study, the procedures involved, the voluntary nature of your organisation's participation, and the confidentiality and anonymisation measures in place. You also confirm that you have the authority to consent on your organisation's behalf.
Authorized Representative Name: _____ Authorized Representative Signature: _____ Date: _____ Researcher's Signature: _____ Date: _____

APPENDIX B

B.1 Sample of Risk-Based Assessment Kit

B.1.1 One Sample Ability Control Question for Each Ability Section

Abilities	Ability Control Metrics	Risk Score of the Controls (Out of 5)	Ability Control Questions	Yes	No	Pro of Documents	Risk Score of the Organization by the Controls	Risk Score Explanation & Necessity Arguments	Control Reference
Policy	A policy has been put in place for information security within the organization		Does the organization have an information security policy in place that outlines the organization's approach to protecting sensitive information?			The existence of an information security policy includes a written policy document that outlines the organization's approach to protecting	0	Having a well-defined information security policy is crucial as it sets the foundation for an organization's security posture. It outlines the organization's commitment to protecting sensitive information and provides a framework for implementing security controls.	NIST CSF: PR.AC-1, PR.AC-2 ISO 27001:2013: Clause 5 HIPAA: 164.308(a)(5) COBIT 5: PO10.1 COBIT 2019: PO5.3 GDPR: Article 24

						sen siti ve inf or mat ion.			
Access Control (Physical)	Security measures have been implemented to restrict physical access to data centers and device closets that host IT infrastructure and application servers.		Are access to data centers and device cabinets restricted to authorized personnel only?			Ac ces s to dat a cen ters and dev ice cab inet s is rest rict ed to aut hor ize d per son nel only incl ude s acc ess con trol list s and oth er doc um ent atio n that outl ine the indi vid ual s or gro ups that are aut hor	0	Restricting access to authorized personnel helps limit unauthorized access but doesn't address insider threats or other security risks.	FISMA:SP 800-53 Rev.4: AC-6(1) Physical Access Control HIPAA:164.312(b)(1): Facility access controls FERMA:chapter 5: Physical security GLBA:Title V: Physical Safeguards SOX:404: Internal Control over Financial Reporting ITIL:ITIL 4 - Continual Improvement COBIT 2019:APO12.03: Manage Physical Access Control SOC 2:SOC 2 - Physical Security PCI DSS:Requirement 9: Physical security GDPR:Article 32: Security of processing NIST SP 1800-35:Section 5: Physical Security NIST SP 800-171: Physical Security NIST SP 800-53 Rev.4: Physical and Environmental Protection

						ize d to acc ess the dat a cen ters and dev ice cab inet s..			
Laws&Re - gulations	The laws and regulations related to cybersecurity, including responsibilities related to privacy and civil liberties, are comprehended and effectively addressed.		Are there designated individuals or teams responsible for ensuring compliance with legal and regulatory requirements for cyber security?			Do cu me ntat ion that outl ine s the role s and res pon sibi lities of indi vid ual s or tea ms res pon sibl e for ens uri ng co mpl ian ce wit h leg al and reg ulat ory req uire me nts. Thi	0	Designated individuals help ensure compliance but do not guarantee effective security measures.	NIST CSF: ID.RA-1 "Identify and document legal, regulatory, and organizational requirements for protecting PII and other sensitive information" FISMA: Title III, Subtitle A "Federal Information Security Modernization Act of 2014" HIPAA: § 164.308(a)(7) "Security management process" FERMA: "Compliance with legal and regulatory requirements" GLBA: Title V, Subtitle A "Privacy" SOX: Section 404 "Internal Control over Financial Reporting" ITIL: "Compliance and legal" COBIT 2019: PO5.2 "Ensure legal and regulatory compliance" SOC 2: "Legal and regulatory compliance" PCI DSS: "Compliance

						s doc um ent atio n cou ld incl ude job des crip tion s, org ani zati ona l cha rts, or oth er doc um ent atio n that sho ws ho w co mpl ian ce res pon sibi litie s are dist rib ute d acr oss the org ani zati on.			with legal and regulatory requirements" GDPR: "Compliance with legal and regulatory requirements" NIST SP 1800-35: "Legal and regulatory compliance"
Inventory & Asset Management (Physical Devices)	A record is maintained of all physical devices and systems present within the		Are there processes in place to detect and respond to physical security breaches,			Do cu me ntat ion that outl ine	0	Processes to detect and respond to breaches contribute to overall security but don't prevent	NIST CSF: Identify (ID) - ID.AM-2 - Physical Asset Management FISMA: Security Control 3.3 - Physical and

	organization.		including unauthorized access or tampering of devices and systems?			s pro ced ure s for det ecti ng and res pon din g to phy sica l sec urit y bre ach es, suc h as an inci den t res pon se pla n or sec urit y inci den t ma nag em ent pro ced ure s. The doc um ent atio n sho uld sho w that the org ani zati on		breaches from happening.	Environmental Protection HIPAA: 164.308(a)(4)(ii)(B) - Implement physical safeguards for all workstations that access electronic protected health information FERMA: Section 9.2.2 - Physical security GLBA: Title V, Subtitle A, Part 501 - Information Security SOX: IT General Controls - Physical and Environmental Protection ITIL: ITIL V4 - Continual Service Improvement - Service Asset and Configuration Management COBIT 2019: Governance and Management - IT Asset Management SOC 2: Security - Physical and Environmental Protection PCI DSS: Requirement 9 - Physical and Environmental Security GDPR: Article 32 - Security of processing
--	---------------	--	--	--	--	---	--	--------------------------	---

						has established procedures to identify and respond to physical security breaches, including unauthorized access or tampering of devices and systems.			
Asset Management (Lifecycle)	Assets are systematically tracked and managed through their entire lifecycle, including disposal, transfer, and removal		Are there processes in place to verify that data has been erased or destroyed on devices that are no longer in use?			Documentation that outlines the procedures for verifying that data	0	Verifying data erasure and destruction contributes to overall security but doesn't prevent unauthorized access.	NIST CSF: ID.AM-4, ID.AM-5 NIST SP 800-53: AC-11, AC-12, AC-13 ITIL: ITIL 4: Continual Improvement > Continual Improvement COBIT 2019: Governance and Management > IT Asset Management > IT Asset Management COBIT 5: "Process"

						a has been erased or destroyed on devices that are no longer in use. This documentation should show that the organization has established procedures for verifying that data has been securely erased or destroyed		Domain, specifically the "DSS05 - Manage the IT Asset Lifecycle" process. SOC 2: Security > Asset Management PCI DSS: Requirement 6.1, 6.3 GDPR: Article 32: Security of Processing NIST SP 1800-35: Guide for Managing the Security of Mobile Devices in the Enterprise > Mobile Device Security Management Program > Mobile Device Life Cycle Management > Retirement and Disposal of Mobile Devices ISO/IEC 27001:2013, in the "Asset management" section. ISO/IEC 27002:2013, in the "Information security management" section.
--	--	--	--	--	--	---	--	--

						, such as conducting tests or inspections. Organizational charts or job descriptions to ensure that there are designated individuals or teams responsible for compliance.			
Security Threat Management	The organization's risk management and governance processes are designed to mitigate the risks associated with		Is there a incident response plan in place for dealing with ransomware attacks and how often it is tested and updated?			Organization's incident response plan and inci	0	Incident response plans help mitigate ransomware attacks but don't guarantee prevention.	NIST CSF: PR.AC-1: Access Control Policy and Procedures PR.AC-2: Account Management PR.AC-3: Access Control PR.AC-4: Identification and Authentication PR.AC-5: Authorization

	ransomware					den t res pon se test ing rep orts to ens ure that the pla n is in pla ce for dea ling wit h ran so mw are atta cks. Exa min e inci den t rep orts to ass ess wh eth er the org ani zati on is foll owi ng the inci den t res pon se pla n and test		PR.AC-6: Least Privilege PR.AC-7: Separation of Duties PR.MG-1: Risk Management Policy and Procedures PR.MG-2: Risk Assessment PR.MG-3: Risk Mitigation PR.MG-4: Risk Monitoring and Reporting FISMA: AC-6: Least Privilege AC-16: Separation of Duties RM-1: Risk Management Policy and Procedures RM-2: Risk Assessment RM-3: Risk Mitigation RM-4: Risk Monitoring and Reporting HIPAA: 164.308(a)(1): Security Management Process 164.308(a)(7): Security Incident Procedures 164.308(a)(8): Contingency Plan 164.308(a)(9): Evaluation 164.308(b)(1): Facility Access controls 164.308(b)(2): Access Control and Validation Procedures FERMA:Section 4: Risk Management GLBA: Title V: Privacy of Consumer Financial Information Title V, Subtitle A: Financial Privacy
--	------------	--	--	--	--	---	--	---

						ing it reg ular ly.		SOX:Section 404: Management Assessment of Internal Control ITIL: ITIL Service Design: Service Design Processes ITIL Service Transition: Change Management ITIL Service Operation: Incident Management ITIL Continual Service Improvement: Service Level Management COBIT 2019: PO5.6, PO5.7, PO5.8, PO5.9, PO5.10, PO5.11, PO5.12, PO5.13 GDPR: Article 32
Vulnerability Identification	A record is created identifying the vulnerabilities present in the assets within the organization		Are there regular reviews of the organization's inventory of assets to ensure that all assets are accounted for and that any newly added assets are also assessed for vulnerabilities?			Evidence records of asset inventory and vulnerability assessments to ensure that the organization regularly reviews its	0	Regular inventory reviews contribute to overall security but don't directly address cyber threats. NIST CSF: ID.AM-1: Asset Management Policy and Procedures ID.AM-2: Inventory of Authorized and Unauthorized Devices ID.AM-3: Inventory of Authorized and Unauthorized Software ID.AM-4: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers ID.AM-5: Boundary Defense ID.AM-6: Maintenance, Monitoring, and Analysis of Audit Logs NIST SP 1800-35: Section 5.1.1: Asset

						inventory of assets and assess newly added assets for vulnerabilities. Additionally, reviewing incident reports to assess whether the organization's asset inventory is accurate and up-to-date.			Management Policy and Procedures Section 5.1.2: Identification and Authentication of Assets Section 5.1.3: Inventory of Authorized and Unauthorized Devices Section 5.1.4: Inventory of Authorized and Unauthorized Software Section 5.1.5: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers Section 5.1.6: Boundary Defense Section 5.1.7: Maintenance, Monitoring, and Analysis of Audit Logs NIST SP 800-53: "Security and Privacy Controls for Federal Information Systems and Organizations" recommends organizations to identify and document vulnerabilities in the organization. ISO 27001:2013: Clause 6 PCI DSS: Requirement 11.2
Vulnerability Management	The organization has created and		Are all third-party software and			Evidence rec	0	Checking third-party software and services for	NIST CSF: -PR.DS-1: Identify and document the

	put into action a plan for managing vulnerabilities		services used by the organization regularly checked for vulnerabilities?			ords of third-party software and service assessments to ensure that they are regularly checked for vulnerabilities. Additionally, reviewing contracts or agreements with third-party vendors to assess whether		vulnerabilities is crucial but doesn't guarantee complete security.	organization's critical information and the associated assets -PR.DS-2: Prioritize and scope the organization's information and information systems for protection -PR.DS-3: Assess and authorize information systems -PR.DS-4: Continuously monitor and protect organizational information and information systems -PR.DS-5: Respond to detected cybersecurity incidents -PR.DS-6: Recover from cybersecurity incidents -PR.DS-7: Implement sub-controls for specific types of information and systems FISMA: -AC-2: Security Categorization -AC-7: Incident Response Capability -AC-17: Incident Response and Reporting HIPAA: -164.308(a)(8) Security Management Process -164.308(a)(7) Incident Procedures -164.308(a)(6) Access Control -164.308(a)(5) Security Awareness and Training
--	---	--	--	--	--	--	--	---	--

						er the y incl ude pro visi ons for vul ner abil ity ma nag em ent.		FERMA: -Risk Management Methodology -Information Security Management -Business Continuity Management GLBA: -501(b) Standards for safeguarding customer information SOX: -404: Management assessment of internal controls ITIL: -Service Operation -Continual Service Improvement COBIT 2019: -DS5.11: Manage vulnerabilities -DS5.12: Manage security incidents and events -DS5.13: Manage security information and event management (SIEM) SOC 2: -Security -Availability -Processing integrity -Confidentiality -Privacy PCI DSS: 6.1: - Establish a process to identify vulnerabilities ISO 27001:2013: - Clause 6.1.2 "Risk assessment and treatment" NIST SP 800-53: - RA-5 "Vulnerability management" - SOC 2: CA-2 "Vulnerability management"
--	--	--	--	--	--	--	--	---

								PCI DSS: Section 6.1 "Install and maintain a firewall configuration to protect cardholder data" COBIT 5: Process PO4 "Manage service level"
Continuous Vulnerability Scan	Regular vulnerability scanning is conducted		Are the results of the vulnerability scans and penetration tests reviewed and actioned in a timely manner?			Requesting evidence of how vulnerabilities discovered during scans and tests were addressed, such as documented evidence of patching and remediation activities.	0	Timely review and action on scan and test results is important but doesn't guarantee complete security. NIST SP 800-53 Rev. 4: This standard includes a control for "Vulnerability Scanning" which requires that organizations conduct regular vulnerability scans to identify vulnerabilities in their systems and networks. ISO/IEC 27001:2013: Requirements - This standard specifies requirements for an information security management system (ISMS) and includes a section on vulnerability management which requires organizations to conduct regular vulnerability assessments to identify vulnerabilities in their systems and networks. SOC 2: This standard requires that service providers implement appropriate controls to protect client data, including regular vulnerability scanning to identify vulnerabilities in their systems and

								networks. PCI DSS: This standard requires that organizations conduct regular vulnerability scans to identify vulnerabilities in their systems and networks that are connected to the cardholder data environment. OWASP: This organization provides guidance on web application security, including the need to conduct regular vulnerability scans to identify vulnerabilities in web applications. NIST SP 800-115 Technical Guide to Information Security Testing and Assessment: This guide provides recommendations for security testing and assessment, including the need to conduct regular vulnerability scans to identify vulnerabilities in systems and networks.
Network Segmentation	The security of the network is maintained, and network segregation is implemented where necessary to ensure network integrity		Are there network segmentation and isolation measures in place to limit the potential impact of a security incident on the organization's network?			Evidence of the network segmentation and isolation measure	0	Network segmentation and isolation help limit the impact of incidents but don't prevent incidents from happening. NIST CSF: ID.SC-13, ID.SC-14, ID.SC-15, ID.SC-16, PR.IP-1, PR.IP-2 NIST SP 800-53: AC-17 (Network Segmentation), AC-18 (Boundary Defense), SI-4 (Network Boundary Protection) NIST SP 1800-1: 18.5.1, 18.5.2,

						as res in pla ce to lim it the pot enti al imp act of a sec urit y inci den t on the org ani zati on's net wor k.			18.5.3, 18.5.4 PCI DSS: Requirement 1.3.7, 1.3.8, 1.3.9, 1.3.10, 1.3.11 SOC 2: Security Principle 2.1, 2.2, 2.3, 2.4, 2.5 HIPAA: 164.312(a)(2)(ii), 164.312(a)(2)(iii) FERMA: Risk Management, IT Security, IT Governance, IT Compliance GLBA: Title V, Section 501, 503 SOX: Section 302, 404 ITIL: IT Service Continuity Management, IT Security Management, IT Operations Management COBIT 2019: IT- 04, IT-07, IT-08, IT-09, IT-10 GDPR: Article 32, Article 33
User Managem ent	Processes are established for on- boarding and off- boarding user access.		Are there automated procedures for revoking access for terminated employees or contractors and removing them from the IAM source?			Evi den ce of the aut om ate d pro ced ure s for rev oki ng acc ess for ter min ate d em plo yee s or con trac tors			NIST CSF: PR.AC-5, PR.AC-6, PR.AC-7, PR.AC-8 FISMA: AC-6, AC-7, AC-8, AC-9, AC-10 HIPAA: 164.308(a)(4), 164.308(a)(5), 164.308(a)(6), 164.308(a)(7), 164.308(a)(8), 164.308(a)(9), 164.308(a)(10), 164.308(a)(11) PCI DSS: 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8 ISO 27001:2013: Clause 8
							0	Automated procedures for revoking access are important but don't guarantee complete security.	

						, such as user account management processes and termination checklists.			
Data-at-rest	Protection of data-at-rest		Are there measures in place to detect and respond to potential data breaches, such as data loss prevention (DLP) systems and incident response plans?			Requesting evidence of the measures in place to detect and respond to potential data breaches, such as documented DLP policies,	0	Detection and response measures for potential data breaches contribute to overall security but don't guarantee complete security.	NIST CSF: ID.AM-1, ID.AM-2, ID.AM-3 NIST SP 800-53: CP-2, CP-3, CP-4, CP-5, CP-6, CP-7, SC-28 HIPAA: 164.312(a)(2), 164.312(b), 164.312(c)(1) COBIT 2019: DS5.1 SOC 2: N/A PCI DSS: 3.5, 3.5.1, 3.5.2, 3.5.3, 3.5.4 GDPR: Article 32 ISO/IEC 27001:2013: "Security management" and "Access control" sections.

						pro ced ure s, and inci den t res pon se pla ns.		
Data-in- transit	Protection of data-in- transit		Are there processes in place to ensure that all third party connections to the organizatio n's network are properly secured, and data-in- transit are protected when transmitted to/from these third parties?			Evi den ce of pro ces ses in pla ce to ens ure that all thir d part y con nec tion s to the org ani zati on's net wor k are pro perl y sec ure d and dat aint ran sit are pro tect ed wh en tran smi	0	Third-party connections are secured but there might be room for improvement.
								NIST CSF: ID.AM-1: Automated mechanisms are in place to detect and report/block unauthorized access attempts to network and system resources. ID.AM-2: Automated mechanisms are in place to detect and report/block unauthorized access attempts to network and system resources. ID.RA-1: Remote access to organization's networks and systems is limited to authorized users and devices. ID.RA-2: Remote access to organization's networks and systems is limited to authorized users and devices. ID.RA-3: Remote access to organization's networks and systems is limited to authorized users and devices. ID.SC-7: Cryptographic mechanisms are used to protect the integrity of communications. ID.SC-8: Cryptographic

						tted to/from the third parties, such as third party risk assessment reports and contracts.		mechanisms are used to protect the confidentiality of communications. FISMA: AC-17: Remote access is restricted to authorized individuals. AC-18: Remote access sessions are auditable. AC-19: Remote access is terminated when no longer needed. AC-20: Remote access is encrypted. HIPAA:164.312(e)(2): Standard: Transmission security. FERMA:Section 4.3.3: Remote access. GLBA:Title V, Subtitle A, Part 501: Information Security Standards. SOX:Section 302: Corporate responsibility for financial reports. ITIL: Service Design: Design of secure networks Service Operation: Secure networks Continual Service Improvement: Secure networks NIST SP 800-53 Rev. 4, in the "Security and Privacy Controls for Federal Information Systems and Organizations" control family, specifically the "Communication s Protection" family. ISO/IEC 27001:2013, in
--	--	--	--	--	--	---	--	---

									the "Communication s security" section. PCI DSS, in section 4: Encrypt transmission of cardholder data across open, public networks SOC 2: "Security" criteria under the "Trust Services Criteria" section.
Data Security	Measures to prevent data leakage are put in place		Are these endpoint agents and SaaS/PaaS solutions configured to detect and prevent data leakage?			Evidence of how the endpoint agents and SaaS/PaaS solutions are configured to detect and prevent data leakage, such as configuration documentation and	0	Configurations are set to detect and prevent data leakage but they may not cover all scenarios.	NIST SP 800-53 Rev. 4, in the "Security and Privacy Controls for Federal Information Systems and Organizations" control family, specifically the "Access Control" and "Audit and Accountability" families. ISO/IEC 27001:2013: "Access control" and "Monitoring, analysis and evaluation" sections. PCI DSS: section 10: Track and monitor all access to network resources and cardholder data HIPAA: Security Rule, in the "Implementation specification" for "Access control and validation procedures". SOC 2: "Security" criteria under the "Trust Services Criteria" section. GDPR: Article 32 - Security of processing

						monitoring reports.			
Secure Development	The production environment is kept separate from the development and testing environments		Are there specific security controls in place such as firewall rules, access controls, and encryption to ensure that the access to the development and testing environments is strictly controlled and that data is protected in these environments?			Evidence of the specific security controls in place to ensure that the access to the development and testing environments is strictly controlled and that data is protected in the environments,	0	Security controls are in place but there could be room for enhancement.	NIST CSF: -PR.DS-1: Data Separation -PR.DS-2: Development, Test, and Production Environments -PR.DS-3: Release Management FISMA: -System Development Life Cycle (SDLC) -System Development Life Cycle (SDLC) Policy and Procedures HIPAA: - 164.308(a)(7)(ii)(C): Security management process - 164.308(a)(7)(ii)(D): Information access management NIST SP 800-53 Rev. 4: "Security and Privacy Controls for Federal Information Systems and Organizations" control family, specifically the "Configuration Management" family, ISO/IEC 27001:2013: "Asset management" section. SOC 2: "Security" criteria under the "Trust Services Criteria" section OWASP Top 10: A9 - Using

						such as firewall configuration and access control policies.			Components with Known Vulnerabilities
Change Management	Processes are established to control configuration changes		Are there regular reviews of the configuration change process to ensure that it is operating effectively and that changes are being properly controlled?			Evidence of the regular reviews of the configuration change process to ensure that it is operating effectively and that changes are being properly controlled, such as	0	Reviews are conducted but they may not be exhaustive.	NIST CSF: ID.CM-1: Inventory of Authorized and Unauthorized Devices ID.CM-2: Inventory of Authorized and Unauthorized Software ID.CM-3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers ID.CM-4: Continuous Vulnerability Management ID.CM-5: Controlled Use of Administrative Privileges ID.CM-6: Maintenance, Monitoring, and Analysis of Audit Logs ID.CM-7: Account Monitoring and Control FISMA: AC-2: Security Configuration Management AC-3: Contingency Planning AC-4: Incident Response and Reporting AC-5:

						nge ma nag em ent revi ew rep orts 		Compliance AC-6: Least Privilege AC-7: Security-Focused Configuration Management of Information Systems AC-16: Separation of Duties HIPAA: 164.308(a)(5): Security Management Process 164.308(a)(7): Security Incident Procedures 164.308(a)(8): Contingency Plan 164.308(a)(9): Evaluation 164.308(b)(1): Facility Access Controls 164.312(a)(2): Access Authorization 164.312(a)(5): Auditing and Accountability FERMA: Risk Management Process Incident Management Process Business Continuity Management GLBA: Title V, Subtitle A, Section 501: Information Security Program Title V, Subtitle A, Section 502: Information Security Management SOX:Section 302: Corporate Responsibility for Financial Reports ISO 27001:2013: Clause 6.1.3 "Control of changes" NIST SP 800-53:
--	--	--	--	--	--	--	--	---

									CM-3 "Configuration management" SOC 2: AICPA's Trust Service Principles, CC5.C "Change management process" PCI DSS: section 6.3 "Protect cardholder data" COBIT 5: PO9 "Manage changes" ITIL: "Change management"
Backup & Recovery	Data is periodically backed up, maintained, and tested for reliability		Are there processes in place for testing the recoverability of backups?			Evidence of the processes in place for testing the recoverability of backups, such as documented backup testing protocols and procedures.	0	Backup recoverability tests are performed but they might not cover all scenarios.	NIST CSF: ID.CP-6: Data Backup and Recovery FISMA: NIST SP 800-53 Control: AC-2(2) - ACCOUNT MANAGEMENT - ACCOUNT ACCESS ENFORCEMENT HIPAA: 164.308(a)(7)(ii)(B) - Data Backup Plan ITIL - ITIL 4:Continual Improvement COBIT 2019: DS5.1 Ensure Data Backup and Recovery PCI DSS: Requirement 3.2 - Protect Stored Cardholder Data GDPR: Article 32 - Security of Processing ISO 27001:2013: Clause 9.4 "Backup" NIST SP 800-53: CP-6 "Backup" SOC 2: BC-4 "Backup and recovery" PCI DSS: Section 10.7 "Track and monitor all access to network resources and cardholder data"

									COBIT 5: PO3 "Manage operations" ITIL: Process of "Service continuity management"
Service Level Agreements	Agreements incorporate provisions outlining data ownership and transferability.		Are there contingencies in place in the event that the SLAs for response and notification times for availability and security events are not met? (<u>If yes please select "NO"</u>)			Evidence of the contingencies in place in the event that the SLAs for response and notification times for availability and security events are not met, such as incident response plans and esc	0	Contingencies exist but there might be room for improvement.	ISO 27001:2013: Clause 8.2.2 "Service delivery" NIST SP 800-53: PM-9 "Service level management" that ensures that SLAs are being met, and that regular reporting is performed to track performance against SLAs. SOC 2: AT-3 "Monitoring and reporting" ITIL: Process of "Service level management" COBIT 5: Process PO4 "Manage service level"

						alat ion pro cedure s.			
Vendor Managem ent	Conduct IT vendor risk assessments periodically , with a frequency of at least once every two years for vendors that host or process data.		Are there processes in place for regularly reviewing and assessing the security controls of vendors and third-party service providers used by the organizatio n?			Evi den ce of the pro ces ses in pla ce for reg ular ly revi ewi ng and ass essi ng the sec urit y con trol s of ven dor s and thir dpar ty ser vic e pro vid ers use d by the org ani zati on, suc h as ven dor sec urit y ass	0	Security control assessments are conducted but there could be gaps in coverage.	NIST CSF: ID.SC-13 (Supply Chain Risk Management) FISMA: NIST SP 800-161 (Supply Chain Risk Management) HIPAA: 164.308(a)(8) (Business Associate Contracts and Other Arrangements) GLBA: Title V, § 501(b) (Service Provider Due Diligence) SOC 2: Trust Services Criteria for Security (T5) PCI DSS: 12.8 (Monitor and Test Third-Party Service Provider) GDPR: Art. 32(4) (Security of Processing) NIST SP 1800- 35: SP 1800-35A (Guideline for Vendor Selection, Management, and Coordination) ISO 27001:2013: Clause 6.1.2 "Risk assessment and treatment" NIST SP 800-53: SA-3 "Third- Party security" COBIT 5: Process PO2 "Manage suppliers" ITIL: Process of "Vendor management"

						ess me nt rep orts and doc um ent atio n.			
Log Managem ent	Procedures for determining , documentin g, implementi ng, and reviewing audit and log records are in place in accordance with organizatio nal policies		Are there processes in place for preserving and retaining audit/log records for a specified period of time in accordance with the regulatory requirement s?			Evi den ce of the pro ces ses in pla ce for pre serv ing and reta inin g aud it/l og rec ord s for a spe cifi ed peri od of tim e in acc ord anc e wit h reg ulat ory req uire me nts, suc h as aud it	0	Preservation and retention processes exist but there might be room for improvement.	NIST CSF: -PR.DS-1: Data Protection -PR.DS-2: Data Protection Through Access Control -PR.DS-3: Data Protection Through Network Segmentation -PR.DS-4: Data Protection Through Encryption -PR.DS-5: Data Protection Through Secure Data Disposal -PR.DS-6: Data Protection Through Incident Response FISMA: -AU-2: Audit and Accountability -AU-3: Auditable Events -AU-4: Audit Review, Analysis, and Reporting -AU-5: Audit Reduction and Report Generation -AU-6: Auditable Alarms -AU-7: Audit Collection from Information Systems HIPAA: -164.312(b) Audit controls -164.312(c)(1) Integrity -164.312(c)(2) Person or entity authentication -164.312(c)(3)

						log rete ntio n poli cies and doc um ent atio n.		Transmission security -164.312(d) Audit procedures -164.312(e)(2) Transmission security FERMA: -R7-1.4: Auditing -R7-1.5: Auditing - Data Protection -R7-1.6: Auditing - Network Segmentation -R7-1.7: Auditing - Encryption -R7-1.8: Auditing - Secure Data Disposal -R7-1.9: Auditing - Incident Response GLBA: -314.4 Service provider due diligence -314.5 Service provider contracts -103(a)(1) Record retention SOX:404. Auditing internal control over financial reporting ITIL: -Service Operation > Event Management > Event Management Process -Service Operation > Incident Management ISO 27001:2013: Clause 10.2.1 "Audit logging" NIST SP 800-53: SI-4 "Audit and accountability" SOC 2: AU-3 "Audit logs" PCI DSS: Section 10.2
--	--	--	--	--	--	---	--	---

								"Review logs and security events for all system components" COBIT 5: PO11 "Monitor and evaluate" ITIL: Process of "Service operation"
Endpoint Security Management	Anti-virus software is installed across the entire system environment		Is an antivirus or EDR/XDR solution currently in use within the organization?			Evidence of an anti virus or EDR/XDR solution currently in use within the organization, such as anti virus software and documentation.	0	Antivirus or EDR/XDR solutions are in use but their coverage may not be complete.
								NIST CSF:Identify (ID.AM-4) - Malware Defenses FISMA:SP 800-53 Rev. 4 - Security and Privacy Controls for Federal Information Systems and Organizations - AC-17: Malware Defenses HIPAA:164.308(a)(5)(ii)(B) - Technical Safeguards - Implementation specifications: Access control and validation procedures COBIT 2019:PO7.4 - Protect and Monitor Information Assets PCI DSS:Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs ISO 27001:2013: Clause 6.1.2 "Risk assessment and treatment" NIST SP 800-53: SI-7 "Malware protection" SOC 2: AT-4 "Malware protection" PCI DSS: Section 11.2 "Regularly test security systems and processes"

									COBIT 5: Process PO5 "Manage IT operations" ITIL: Process of "Service operation"
External network Managem ent	Access to external network entry points is restricted.		Are any external IP addresses or ranges explicitly blocked from accessing the organizatio n's remote control services?			Evi den ce of ext ern al IP add ress es or ran ges exp licit ly blo cke d fro m acc essi ng the org ani zati on's rem ote con trol ser vic es, suc h as fire wal l rule s and net wor k dia gra ms.	0	External IP blocks are in place but there could be gaps.	ISO 27001:2013: Clause 9.2 "Protection of networks" NIST SP 800-53: SC-7 "Boundary protection" SOC 2: AT-2 "Firewall" PCI DSS: Section 1.2.2 "Implement a firewall to protect cardholder data" COBIT 5: Process PO3 "Manage network services" ITIL: Process of "Service operation"
Data Protection	Sensitive files that might be taken offsite from the		Are the organizatio n's critically sensitive documents			Evi den ce that the org	0	Sensitive documents are encrypted but there might be room for enhancement.	NIST CSF: -PR.DS-1: Data Protection and Privacy (encryption used in data storage

	company's premises are safeguarded using readily available encryption tools.		protected by encryption?			an organization's critical sensitive documents are protected by encryption, such as encryption policies and procedures.		and transmission) -PR.DS-2: Data Protection and Privacy (encryption key management) -PR.DS-3: Data Protection and Privacy (encryption of data-at-rest) -PR.DS-4: Data Protection and Privacy (encryption of data-in-transit) -PR.DS-5: Data Protection and Privacy (use of cryptographic modules) -PR.DS-6: Data Protection and Privacy (verification of cryptographic integrity) FISMA: FIPS 200: Minimum Security Requirements for Federal Information and Information Systems (encryption used in data storage and transmission) HIPAA: 45 CFR 164.312(a)(2)(iv) : Technical Safeguards (encryption and decryption) COBIT 2019: -DS5.13: Encryption of Data in Transit -DS5.14: Encryption of Data at Rest -DS5.15: Encryption Key Management -DS5.16: Cryptographic Control PCI DSS: -Requirement 3: Protect stored cardholder data (encryption of cardholder data-at-rest)
--	--	--	--------------------------	--	--	---	--	---

								-Requirement 4: Encrypt transmission of cardholder data across open, public networks GDPR: Article 32(1): Security of processing (encryption) NIST SP 1800-35: - Recommendation 1: Use of Encryption - Recommendation 2: Encryption Key Management - Recommendation 3: Cryptographic Algorithm Implementation - Recommendation 4: Cryptographic Module Implementation
Cybersecurity Organizational Duties	Designate a person within the organization who is responsible for cybersecurity matters.		Are the person or team responsible for cyber security reporting to appropriate level of management and are they held accountable for ensuring the security of the organization?			Evidence that the person or team responsible for cyber security is reporting to appropriate levels of management	0	The cyber security team reports to management and is held accountable but there might be room for improvement. NIST CSF: Identify (ID) Protect (PR) Detect (DE) Respond (RS) Recover (RE) FISMA: Security Management (PL-2) Security Assessment and Authorization (PL-3) Security Certification (PL-4) Continuous Monitoring (PL-5) HIPAA: Security Management Process (164.308(a)(1)) Risk Analysis (164.308(a)(1)(ii)(A)) Risk Management (164.308(a)(1)(ii)(B)) Sanction Policy

						ement and is held accountable for ensuring the security of the organization, such as performance review records and incident response reports.			(164.308(a)(2)) Information System Activity Review (164.308(a)(5)) FERMA: Governance and organization Risk management Compliance Business continuity management Incident management GLBA: Security Management (501.1) Risk Analysis (501.2) Security Program (501.3) Service Provider Arrangements (501.4) Other Standards (501.5) SOX:Section 404: Management's responsibility for internal control ITIL: ITIL service operation ITIL service transition COBIT 2019: DS5: Manage IT governance and IT management DS5.1: Define and manage IT governance DS5.2: Manage the IT portfolio DS5.3: Manage relationships with stakeholders NIST SP 800-53 Rev. 4: Access Control Policy and Procedures ISO/IEC 27001:2013: Requirements
Network Management	Continuous monitoring of the network is in place to identify any		Are the logs from the network controls being regularly			Evidence that the log	0	Logs from network controls are reviewed and retained but there might be	NIST SP 800-53 Rev. 4: "Security Continuous Monitoring" ISO/IEC 27001:2013:

	potential cybersecurity incidents		reviewed, analyzed and retained for a sufficient period of time?			s from the network controls are regularly reviewed, analyzed, and retained for a sufficient period of time, such as log management policies and procedures and audit reports.		room for enhancement in the process.	Requirements SOC 2: This standard requires that service providers implement appropriate controls to protect client data, including monitoring of networks for security events. PCI DSS: This standard requires that organizations implement a process for detecting and responding to security incidents, including the monitoring of networks for potential security events. HIPAA: This law requires that organizations implement technical safeguards to protect electronic protected health information, including the monitoring of networks for potential security events. GDPR: This regulation requires that companies implement appropriate technical and organizational measures to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, including network monitoring to detect potential
--	-----------------------------------	--	--	--	--	---	--	--------------------------------------	---

								security events. COBIT: This framework provides guidance on IT governance and management and includes a section on monitoring and log management which requires that organizations continuously monitor the system and network to detect security events.
--	--	--	--	--	--	--	--	---



B.1.2 Sample Risk Analysis Section for Risk-Based Assessment Kit

	Questions	Confidentiality	Availability	Integrity	Likelihood or Effectiveness		Control's Risk Score
1	Does the organization have an information security policy in place that outlines the organization's approach to protecting sensitive information?						0
2	Are access to data centers and device cabinets restricted to authorized personnel only?						0
3	Are there designated individuals or teams responsible for ensuring compliance with legal and regulatory requirements for cyber security?						0
4	Are there processes in place to detect and respond to physical security breaches, including unauthorized access or tampering of devices and systems?						0
5	Are there processes in place to verify that data has been erased or destroyed on devices that are no longer in use?						0

B.2 Question Pool for the Risk-Based Assessment Kit

	Ability Control Questions	Proof Documents	Risk Score Explanation
1	Does the organization have an information security policy in place that outlines the organization's approach to protecting sensitive information?	The existence of an information security policy includes a written policy document that outlines the organization's approach to protecting sensitive information. The policy should include information on the security measures that the organization has in place to protect its sensitive information, including access controls, data encryption, and employee training.	Having a well-defined information security policy is crucial as it sets the foundation for an organization's security posture. It outlines the organization's commitment to protecting sensitive information and provides a framework for implementing security controls.
2	Is the information security policy reviewed and updated regularly to ensure it remains current and effective?	The information security policy is regularly reviewed and updated and includes documentation of policy reviews, updates, and version control. This documentation should show that the policy is reviewed and updated at least annually or more frequently if needed, and that the review process involves input from relevant stakeholders.	Regularly reviewing and updating the information security policy is essential to ensure it remains effective in addressing emerging threats and vulnerabilities. However, this control alone does not guarantee that the policy is being followed or enforced.
3	Are all employees and contractors required to review and acknowledge the information security policy as part of their onboarding or training process?	All employees and contractors are required to review and acknowledge the information security policy includes records of employee and contractor onboarding and training processes. This documentation should show that the information security policy is included in the	Requiring employees and contractors to review and acknowledge the information security policy is an important step in promoting security awareness. However, this control does not guarantee that individuals fully understand the policy or will comply with it.

		onboarding or training process, and that employees and contractors are required to review and acknowledge the policy in writing.	
4	Are there processes in place to enforce the information security policy, including regular audits and monitoring for compliance?	There are procedures in place to enforce the information security policy includes records of regular security audits and monitoring for compliance. This documentation should show that the organization conducts regular security audits and monitoring for compliance, and that there are consequences for non-compliance.	Enforcing the information security policy through regular audits and monitoring helps ensure that security controls are effective and compliance is maintained. However, this control does not address the need for continuous improvement and adaptation to emerging threats.
5	Are there incident response and reporting procedures outlined in the information security policy for the event of a security breach or other incident?	There are incident response and reporting procedures outlined in the information security policy includes a documented incident response plan. This documentation should show that the organization has an incident response plan in place, which outlines the steps to be taken in the event of a security breach or other incident, and that employees are trained on how to follow the plan. Additionally, documentation should show that incident reporting procedures are in place to ensure that incidents are reported to the	Having incident response and reporting procedures in place helps organizations effectively manage and mitigate the impact of security incidents. While this control is essential, it does not address the need for proactive measures to prevent security breaches in the first place.

		appropriate parties in a timely manner.	
6	Are there physical access controls in place for the organization's data centers and device cabinets?	Physical access controls are in place includes documentation of the security measures that are in place to control physical access to data centers and device cabinets. This could include security plans, access control lists, and other documentation that outline the controls that are in place.	Physical access controls are important for preventing unauthorized access to sensitive infrastructure but do not address cyber threats.
7	Are the physical access controls, such as locks and security cameras, functioning properly and regularly maintained?	Physical access controls are functioning properly and regularly maintained includes documentation of maintenance and repair schedules for locks and security cameras, and any reports of malfunctions or failures. This documentation should show that the physical access controls are functioning properly and being maintained according to a regular schedule.	Proper functioning and maintenance of access controls is crucial but it doesn't guarantee complete security against all threats.

8	Are access to data centers and device cabinets restricted to authorized personnel only?	Access to data centers and device cabinets is restricted to authorized personnel only includes access control lists and other documentation that outline the individuals or groups that are authorized to access the data centers and device cabinets. Additionally, access logs may be used to show that only authorized personnel have accessed the data centers and device cabinets.	Restricting access to authorized personnel helps limit unauthorized access but doesn't address insider threats or other security risks.
9	Are there any logs or records kept of who enters and exits the data centers and device cabinets?	Logs or records are kept of who enters and exits the data centers and device cabinets includes access logs, security camera footage, or other documentation that tracks who has accessed the data centers and device cabinets. These logs or records should be regularly reviewed and audited to ensure that there is no unauthorized access.	Logs and records of access help in investigations but don't directly prevent unauthorized access.
10	Is there a process in place for responding to and reporting any unauthorized access to the data centers and device cabinets?	There is a process in place for responding to and reporting unauthorized access includes documentation of the incident response plan and any reports of unauthorized access. This documentation should show that there is a defined process in place for responding to unauthorized access, including reporting the incident to the appropriate parties and taking	Processes for responding to unauthorized access incidents help mitigate damage but do not prevent incidents from happening.

		corrective action to prevent future incidents.	
11	Does the organization have a clear understanding of the relevant legal and regulatory requirements for cyber security, including privacy and civil liberties obligations?	Documentation that outlines the legal and regulatory requirements for cyber security, such as laws, regulations, and industry standards, and how they apply to the organization's operations. This documentation could also include any legal or regulatory compliance assessments or audits conducted by the organization.	Understanding legal and regulatory requirements is essential for compliance but does not guarantee effective security measures.
12	Are there processes in place for regularly reviewing and updating the organization's compliance with legal and regulatory requirements for cyber security?	Documentation that outlines the process for regularly reviewing and updating the organization's compliance with legal and regulatory requirements, such as a compliance review schedule or a compliance management plan. The documentation could also include reports of compliance assessments or audits, which demonstrate the organization's commitment to monitoring compliance.	Regular reviews ensure compliance but do not necessarily address all security risks.

13	Are there designated individuals or teams responsible for ensuring compliance with legal and regulatory requirements for cyber security?	Documentation that outlines the roles and responsibilities of individuals or teams responsible for ensuring compliance with legal and regulatory requirements. This documentation could include job descriptions, organizational charts, or other documentation that shows how compliance responsibilities are distributed across the organization.	Designated individuals help ensure compliance but do not guarantee effective security measures.
14	Are there processes in place for addressing and reporting potential breaches of legal and regulatory requirements for cyber security?	Documentation that outlines policies and procedures for addressing and reporting potential breaches of legal and regulatory requirements, such as an incident response plan or a compliance violation reporting process. This documentation could also include records of compliance violation investigations, which demonstrate the organization's commitment to taking breaches seriously.	Addressing and reporting potential breaches is important for compliance and accountability but doesn't guarantee effective security.
15	Are there regular trainings or awareness campaigns for employees on legal and regulatory requirements for cyber security and their role in maintaining compliance?	Documentation that shows the organization provides regular trainings or awareness campaigns to employees on legal and regulatory requirements for cyber security. This could include records of training sessions or attendance logs, as well as communication materials such as emails, newsletters, or posters. The	Training helps raise awareness but doesn't guarantee that employees will act according to regulations.

		documentation should also show that employees understand their role in maintaining compliance and are aware of the potential consequences of noncompliance.	
16	Are all physical devices and systems in the organization properly inventoried and tracked, including regular updates and maintenance?	Documentation of an inventory management system that accurately tracks all physical devices and systems, as well as records of regular updates and maintenance. This documentation should show that the organization has a system in place to keep track of all physical devices and systems and regularly maintains them to ensure they are functioning properly.	Proper inventory and tracking of devices contribute to overall security but don't directly address cyber threats.
17	Are physical devices and systems in the organization properly secured, including the use of security measures such as encryption and secure boot?	Documentation that outlines the security measures that are in place to secure physical devices and systems, such as encryption, secure boot, and physical access controls. The documentation should show that the organization has implemented these security measures to protect physical devices and systems from unauthorized access and tampering.	Securing physical devices and systems helps prevent unauthorized access but doesn't cover all security risks.

18	Are there processes in place to detect and respond to physical security breaches, including unauthorized access or tampering of devices and systems?	Documentation that outlines procedures for detecting and responding to physical security breaches, such as an incident response plan or security incident management procedures. The documentation should show that the organization has established procedures to identify and respond to physical security breaches, including unauthorized access or tampering of devices and systems.	Processes to detect and respond to breaches contribute to overall security but don't prevent breaches from happening.
19	Are there regular penetration testing and vulnerability assessments performed on physical devices and systems to identify and address potential vulnerabilities?	Records of regular penetration testing and vulnerability assessments on physical devices and systems, as well as documentation that outlines the scope and results of these assessments. This documentation should show that the organization regularly assesses physical devices and systems for vulnerabilities and takes appropriate action to address any issues that are identified.	Regular testing and assessments help identify vulnerabilities but don't guarantee that all vulnerabilities will be addressed.
20	Are there disaster recovery and business continuity plans in place to ensure the organization can continue to operate in the event of a physical security incident or disaster?	Documentation of disaster recovery and business continuity plans, as well as records of regular testing and updates to these plans. This documentation should show that the organization has established plans to ensure it can continue to operate in the event of a physical security incident or disaster, and regularly tests and updates these	Disaster recovery plans help organizations maintain operations during incidents but don't prevent incidents from happening.

		plans to ensure they remain effective.	
21	Are there processes in place to ensure that devices that are no longer in use are properly erased or the data inside is properly destroyed?	Documentation of policies and procedures for the proper erasure or destruction of data on devices that are no longer in use. This documentation should show that the organization has established processes for ensuring that sensitive data is not left behind on devices that are no longer needed. Legal and regulatory compliance reports or assessments to verify that the organization is aware of the applicable requirements.	Proper data erasure and destruction prevents unauthorized access to data but doesn't guarantee complete security.
22	Are there regular inventory checks of devices to identify those that are no longer in use?	Documentation that outlines the process for regular inventory checks of devices, as well as records of these checks. This documentation should show that the organization regularly checks its inventory of devices to identify those that are no longer in use. Review the organization's compliance management system, including policies and procedures, to ensure that there is a formal process for regularly reviewing and updating compliance.	Inventory checks help manage devices but don't directly address security risks.

		Compliance reports or assessments to verify that the organization is following the process.	
23	Are there secure processes in place for erasing or destroying data on devices that are no longer in use?	Documentation that outlines the procedures for securely erasing or destroying data on devices that are no longer in use. This documentation should show that the organization has established secure procedures for data destruction, such as using specialized software or physically destroying the devices.	Secure data erasure and destruction processes help protect sensitive data but don't cover all security risks.
24	Are there processes in place to verify that data has been erased or destroyed on devices that are no longer in use?	Documentation that outlines the procedures for verifying that data has been erased or destroyed on devices that are no longer in use. This documentation should show that the organization has established procedures for verifying that data has been securely erased or destroyed, such as conducting tests or inspections. Organizational charts or job descriptions to ensure that there are designated individuals or teams responsible for compliance.	Verifying data erasure and destruction contributes to overall security but doesn't prevent unauthorized access.

25	Are there processes in place to ensure that devices that are no longer in use are disposed of in a secure manner?	Documentation that outlines the procedures for disposing of devices that are no longer in use in a secure manner, such as shredding or recycling. This documentation should show that the organization has established procedures for ensuring that devices are disposed of in a way that does not compromise the security of sensitive data. Incident response plans and security incident management procedures to ensure that there are policies and procedures for addressing and reporting potential breaches. Records of compliance violation investigations to verify that the policies and procedures are being followed.	Secure disposal of devices helps protect data but doesn't directly address other security risks.
26	Are there regular audits or inspections of the organization's data destruction process to ensure compliance with internal policies and external regulations?	Documentation of audits or inspections of the organization's data destruction process, as well as records of any findings or corrective actions taken. This documentation should show that the organization regularly conducts audits or inspections to ensure compliance with internal policies and external regulations related to data destruction. Training records to ensure that employees are receiving regular training on legal and regulatory	Audits and inspections ensure compliance but don't guarantee complete security.

		requirements for cyber security. Interview employees to ensure that they are aware of their role in maintaining compliance and that the training is effective.	
27	Does the organization have a clear and up-to-date process for identifying and assessing ransomware risks?	Risk assessments, vulnerability scans, or penetration testing reports to ensure that the organization has a clear and up-to-date process for identifying and assessing ransomware risks. Examine security logs to identify any previous ransomware incidents and assess whether the organization has taken appropriate steps to mitigate future risks.	Identifying ransomware risks is important but doesn't guarantee prevention of attacks.
28	Are there regular reviews of security controls to ensure they are effective in detecting and preventing ransomware attacks?	Security control review reports, such as firewall configurations, intrusion detection/prevention systems, and anti-virus solutions, to ensure that they are effective in detecting and preventing ransomware attacks. Incident reports to assess whether any ransomware attacks were detected and prevented by these security controls.	Regular reviews of controls help detect and prevent ransomware but don't guarantee complete security.

29	Is there a incident response plan in place for dealing with ransomware attacks and how often it is tested and updated?	Organization's incident response plan and incident response testing reports to ensure that the plan is in place for dealing with ransomware attacks. Examine incident reports to assess whether the organization is following the incident response plan and testing it regularly.	Incident response plans help mitigate ransomware attacks but don't guarantee prevention.
30	Are there regular employee trainings in place to educate staff on how to recognize and respond to potential ransomware attacks?	Review employee training records and security awareness campaigns to ensure that employees are regularly trained on how to recognize and respond to potential ransomware attacks. Interview employees to ensure that they understand their roles and responsibilities in preventing ransomware attacks.	Employee training helps raise awareness but doesn't guarantee that employees will act accordingly.
31	Are there effective measures in place to monitor and detect any unusual activity or unauthorized access on the networks and systems that could indicate a ransomware attack is in progress?	Examine security logs, intrusion detection/prevention systems, and other monitoring tools to ensure that the organization has effective measures in place to detect any unusual activity or unauthorized access that could indicate a ransomware attack is in progress. Examine incident reports to assess whether the organization is following its security monitoring procedures and taking appropriate action when necessary.	Monitoring and detection measures contribute to overall security but don't guarantee ransomware prevention.

32	Are there formal processes in place to identify and document vulnerabilities in the organization's assets, such as systems and applications?	Review of the records of vulnerability assessments, penetration testing, and risk assessments to ensure that the organization has established formal processes for identifying and documenting vulnerabilities in its assets. Also examination of the records of incidents or breaches to assess the effectiveness of these processes.	Identifying vulnerabilities is important but doesn't guarantee all vulnerabilities will be addressed.
33	Are regular vulnerability assessments and penetration testing conducted on the organization's assets to identify vulnerabilities?	Evidence records of vulnerability assessments and penetration testing to verify that they are conducted on a regular basis. Additionally, reviewing the scope and results of these assessments to ensure that vulnerabilities are being identified and addressed.	Regular assessments help identify vulnerabilities but don't guarantee that all vulnerabilities will be addressed.
34	Are identified vulnerabilities tracked and managed through a vulnerability management program?	Evidence records of vulnerability tracking and management to ensure that the organization has established a formal vulnerability management program. Additionally, reviewing records of remediation efforts to assess the effectiveness of the program.	Vulnerability management helps address vulnerabilities but doesn't guarantee complete security.
35	Are critical vulnerabilities addressed in a timely manner and is there a priority ranking system to ensure that the most severe vulnerabilities are addressed first?	Reviewing records of vulnerability remediation to assess whether critical vulnerabilities are being addressed in a timely manner. Additionally, examining the organization's priority ranking	Timely addressing of critical vulnerabilities is important but doesn't guarantee complete security.

		system to ensure that the most severe vulnerabilities are being addressed first.	
36	Are there regular reviews of the organization's inventory of assets to ensure that all assets are accounted for and that any newly added assets are also assessed for vulnerabilities?	Evidence records of asset inventory and vulnerability assessments to ensure that the organization regularly reviews its inventory of assets and assesses newly added assets for vulnerabilities. Additionally, reviewing incident reports to assess whether the organization's asset inventory is accurate and up-to-date.	Regular inventory reviews contribute to overall security but don't directly address cyber threats.
37	Does the organization have a documented vulnerability management program in place?	Reviewing the organization's vulnerability management program to assess whether it is properly documented and formalized. Additionally, examining records of vulnerability tracking, management, and remediation to assess the effectiveness of the program.	A documented vulnerability management program helps manage vulnerabilities but doesn't guarantee complete security.
38	Are there regular scheduled vulnerability scans and assessments performed on the organization's systems and networks?	Evidence records of vulnerability scans and assessments to verify that they are performed on a regular schedule. Additionally, reviewing the scope and results of these scans to assess whether vulnerabilities are being identified and addressed.	Regular vulnerability scans help identify vulnerabilities but don't guarantee that all vulnerabilities will be addressed.

39	Are vulnerabilities identified through scans and assessments promptly prioritized and remediated according to their risk level?	Reviewing records of vulnerability remediation to assess whether vulnerabilities are being prioritized and remediated according to their risk level. Additionally, reviewing incident reports to assess whether the organization is addressing vulnerabilities in a timely manner.	Prioritizing and remediating vulnerabilities is important but doesn't guarantee complete security.
40	Are all third-party software and services used by the organization regularly checked for vulnerabilities?	Evidence records of third-party software and service assessments to ensure that they are regularly checked for vulnerabilities. Additionally, reviewing contracts or agreements with third-party vendors to assess whether they include provisions for vulnerability management.	Checking third-party software and services for vulnerabilities is crucial but doesn't guarantee complete security.
41	Is there a process in place for reporting and tracking vulnerabilities and their resolution?	Reviewing the organization's vulnerability reporting and tracking procedures to ensure that they are properly documented and followed. Additionally, examining records of vulnerability remediation to assess the effectiveness of the reporting and tracking process.	Reporting and tracking processes help manage vulnerabilities but don't guarantee complete security.
42	Are vulnerability scans and penetration tests performed on a regular basis?	Evidence records of vulnerability scans and penetration tests to verify that they are performed on a regular basis. Additionally, reviewing incident reports to assess the effectiveness of these assessments.	Regular scans and tests help identify vulnerabilities but don't guarantee that all vulnerabilities will be addressed.

43	Is there a schedule in place for performing vulnerability scans and penetration tests?	Evidence the documented schedule for these tests and scans, including the frequency and scope of each test. You can also request the reports of previous scans and tests.	Scheduling scans and tests is important but doesn't directly address security risks.
44	Are the results of the vulnerability scans and penetration tests reviewed and actioned in a timely manner?	Requesting evidence of how vulnerabilities discovered during scans and tests were addressed, such as documented evidence of patching and remediation activities.	Timely review and action on scan and test results is important but doesn't guarantee complete security.
45	Is there a process in place for identifying and prioritizing vulnerabilities that are discovered during scans and tests?	Evidence the documented process for identifying and prioritizing vulnerabilities discovered during scans and tests, such as a risk assessment process or a vulnerability management plan.	Identifying and prioritizing vulnerabilities is crucial but doesn't guarantee complete security.
46	Are the findings from vulnerability scans and penetration tests shared with relevant stakeholders, including management and technical teams?	Requesting evidence that the findings from vulnerability scans and penetration tests were shared with relevant stakeholders, including management and technical teams.	Sharing findings is important for collaboration but doesn't directly address security risks.
47	Are there processes in place to prevent unauthorized access or modification to the organization's network?	Requesting evidence of the processes in place to prevent unauthorized access or modification, such as documented security policies, access control lists, and audit logs.	Processes to prevent unauthorized access or modification contribute to overall security but don't guarantee complete security.
48	Are firewalls and other perimeter security controls configured and maintained to protect the organization's network from unauthorized access?	Evidence evidence of how firewalls and other perimeter security controls are configured and maintained, such as change management logs and documentation.	Firewalls and perimeter controls help protect networks but don't guarantee complete security.

49	Are there regular security assessments of the organization's network infrastructure to identify and remediate vulnerabilities?	Evidence evidence of how regular security assessments of the organization's network infrastructure are conducted and documented, such as vulnerability scan reports or penetration test results.	Regular assessments of network infrastructure help identify vulnerabilities but don't guarantee complete security.
50	Are there mechanisms in place to detect and respond to potential network breaches, such as intrusion detection and response systems?	Requesting evidence of the mechanisms in place to detect and respond to potential network breaches, such as network intrusion detection and response systems.	Detection and response mechanisms contribute to overall security but don't guarantee prevention of breaches.
51	Are there network segmentation and isolation measures in place to limit the potential impact of a security incident on the organization's network?	Evidence evidence of the network segmentation and isolation measures in place to limit the potential impact of a security incident on the organization's network.	Network segmentation and isolation help limit the impact of incidents but don't prevent incidents from happening.
52	Are there formal processes in place for provisioning and deprovisioning user access to the organization's systems and applications?	Requesting evidence of the formal processes in place for provisioning and deprovisioning user access, such as user access request forms and approval workflows.	Formal processes for provisioning and deprovisioning access are important but don't guarantee complete security.
53	Are there processes in place to ensure that user access is granted only to those who have a legitimate business need?	Evidence evidence of how the organization ensures that user access is granted only to those with a legitimate business need, such as documented access control policies and procedures.	Ensuring access is granted based on business need helps limit unauthorized access but doesn't address all security risks.
54	Is there an Identity and Access Management (IAM) system in place to manage user access and authentication?	Evidence evidence of the IAM system in place, including documentation of user access controls, authentication mechanisms, and audit logs.	IAM systems help manage user access but don't guarantee complete security.

55	Are there regular reviews of user access to ensure that it is still necessary and appropriate?	Evidence evidence of how the organization conducts regular reviews of user access, such as access review reports and audit logs.	Regular access reviews contribute to overall security but don't directly address cyber threats.
56	Are there controls in place to detect and respond to suspicious or unauthorized access attempts?	Requesting evidence of the controls in place for detecting and responding to suspicious or unauthorized access attempts, such as intrusion detection systems or security incident response plans.	Controls to detect and respond to suspicious access attempts contribute to overall security but don't guarantee complete security.
57	Are there automated procedures for revoking access for terminated employees or contractors and removing them from the IAM source?	Evidence evidence of the automated procedures for revoking access for terminated employees or contractors, such as user account management processes and termination checklists.	Automated procedures for revoking access are important but don't guarantee complete security.
58	Are there processes in place to protect data-at-rest, including encryption and access controls?	Evidence evidence of processes in place to protect dataatrest, such as documented encryption policies, access controls, and data classification.	Protecting data-at-rest with encryption and access controls is important but doesn't guarantee complete security.
59	Is encryption used to protect sensitive data stored on servers, laptops, and other devices?	Requesting evidence of how encryption is used to protect sensitive data stored on servers, laptops, and other devices, such as encryption configuration documentation.	Encryption of sensitive data helps protect it but doesn't guarantee complete security.
60	Are access controls in place to limit access to sensitive data to only authorized individuals?	Evidence evidence of the access controls in place to limit access to sensitive data, such as documented access control policies, procedures, and audit logs.	Access controls help limit unauthorized access but don't guarantee complete security.

61	Are regular backups of sensitive data taken and are they protected using encryption and other security controls?	Evidence evidence of how regular backups of sensitive data are taken and protected, such as backup and recovery procedures and documentation.	Regular backups and protection measures are important but don't guarantee complete security.
62	Are there measures in place to detect and respond to potential data breaches, such as data loss prevention (DLP) systems and incident response plans?	Requesting evidence of the measures in place to detect and respond to potential data breaches, such as documented DLP policies, procedures, and incident response plans.	Detection and response measures for potential data breaches contribute to overall security but don't guarantee complete security.
63	Are there regular security assessments or penetration testing to identify and remediate vulnerabilities in data-at-rest storage systems?	Evidence evidence of regular security assessments or penetration testing to identify and remediate vulnerabilities in dataatrest storage systems, such as vulnerability scan reports or penetration test results.	Assessments and penetration testing of storage systems help identify vulnerabilities but don't guarantee complete security.
64	Are there processes in place to protect data-in-transit, including encryption and secure communication protocols?	Evidence evidence of the processes in place to protect dataintransit, such as documented encryption policies, secure communication protocols, and network security controls.	Protecting data-in-transit with encryption and secure protocols is important but doesn't guarantee complete security.
65	Are secure communication protocols, such as HTTPS and SSL/TLS, used to protect data-in-transit over the network?	Evidence evidence of how secure communication protocols, such as HTTPS and SSL/TLS, are used to protect dataintransit over the network, such as network configuration documentation and certificates.	Secure communication protocols help protect data-in-transit but don't guarantee complete security.
66	Are encryption technologies used to protect sensitive data-in-transit such as VPN and SSH?	Evidence evidence of how encryption technologies are used to protect sensitive dataintransit, such as VPN and SSH	Encryption technologies for sensitive data-in-transit help protect data but don't guarantee complete security.

		configuration documentation.	
67	Are there measures in place to detect and respond to potential data breaches, such as network intrusion detection systems and incident response plans?	Requesting evidence of the measures in place to detect and respond to potential data breaches in dataintransit systems, such as network intrusion detection systems and incident response plans.	Detection and response measures for potential data breaches contribute to overall security but don't guarantee complete security.
68	Are regular security assessments or penetration testing conducted to identify and remediate vulnerabilities in data-in-transit systems?	Evidence evidence of regular security assessments or penetration testing conducted to identify and remediate vulnerabilities in dataintransit systems, such as vulnerability scan reports or penetration test results.	Security assessments and penetration testing of data-in-transit systems help identify vulnerabilities but don't guarantee complete security.
69	Are there processes in place to ensure that all third party connections to the organization's network are properly secured, and data-in-transit are protected when transmitted to/from these third parties?	Evidence evidence of processes in place to ensure that all third party connections to the organization's network are properly secured and dataintransit are protected when transmitted to/from these third parties, such as thirdparty risk assessment reports and contracts.	Third-party connections are secured but there might be room for improvement.
70	Are there endpoint agents and SaaS/PaaS solutions in place to protect against data leakage?	Requesting evidence of the endpoint agents and SaaS/PaaS solutions in place to protect against data leakage, such as configuration documentation and monitoring reports.	Endpoint agents and SaaS/PaaS solutions are in place but their effectiveness could be enhanced.
71	Are these endpoint agents and SaaS/PaaS solutions configured to detect and prevent data leakage?	Evidence evidence of how these endpoint agents and SaaS/PaaS solutions are configured to detect and prevent data leakage, such	Configurations are set to detect and prevent data leakage but they may not cover all scenarios.

		as configuration documentation and monitoring reports.	
72	Are there regular security assessments or penetration testing conducted to evaluate the effectiveness of the endpoint agents and SaaS/PaaS solutions in preventing data leakage?	Evidence evidence of regular security assessments or penetration testing conducted to evaluate the effectiveness of the endpoint agents and SaaS/PaaS solutions in preventing data leakage, such as vulnerability scan reports or penetration test results.	Security assessments are conducted but there could be gaps in coverage.
73	Are there processes in place to respond to incidents of data leakage, including incident response plans and incident management teams?	Evidence evidence of the processes in place to respond to incidents of data leakage, such as incident response plans and incident management teams.	Incident response processes are in place but they could be refined.
74	Are there regular training and awareness programs for employees to educate them on the importance of data security and to prevent data leakage?	Evidence evidence of the regular training and awareness programs for employees to educate them on the importance of data security and to prevent data leakage, such as training materials and attendance records.	Training and awareness programs exist but there's potential for further development.
75	Are there regular monitoring and auditing of logs and system events to detect and prevent data leakage?	Evidence evidence of the regular monitoring and auditing of logs and system events to detect and prevent data leakage, such as monitoring reports and audit logs.	Monitoring and auditing are performed but there might be blind spots.
76	Are there clear separation and isolation between development, testing and production environments to prevent unauthorized access and data leakage?	Evidence evidence of the clear separation and isolation between development, testing, and production environments to prevent unauthorized access and data leakage,	Separation and isolation are implemented but there may be some vulnerabilities.

		such as network configuration documentation and access control policies.	
77	Are there processes in place to ensure that development and testing environments are separate from the production environment?	Evidence evidence of the processes in place to ensure that development and testing environments are separate from the production environment, such as network configuration documentation and access control policies.	Processes are in place but enforcement could be stricter.
78	Are there regular security assessments or penetration testing conducted to evaluate the effectiveness of the separation and isolation between development, testing and production environments?	Evidence evidence of the regular security assessments or penetration testing conducted to evaluate the effectiveness of the separation and isolation between development, testing, and production environments, such as vulnerability scan reports or penetration test results.	Security assessments are conducted but there could be areas for improvement.
79	Are there processes in place to ensure that data and configurations used in development and testing environments do not affect the production environment?	Evidence evidence of the processes in place to ensure that data and configurations used in development and testing environments do not affect the production environment, such as documented change control procedures and testing protocols.	Processes are in place but data and configuration isolation might not be perfect.
80	Are there regular monitoring and auditing of the network and system logs to detect any unauthorized access or data	Evidence evidence of the regular monitoring and auditing of the network and system logs to detect any unauthorized access or data leakage	Monitoring and auditing exist but there may be some areas that are overlooked.

	leakage between development, testing and production environments?	between development, testing, and production environments, such as monitoring reports and audit logs.	
81	Are there specific security controls in place such as firewall rules, access controls, and encryption to ensure that the access to the development and testing environments is strictly controlled and that data is protected in these environments?	Evidence evidence of the specific security controls in place to ensure that the access to the development and testing environments is strictly controlled and that data is protected in these environments, such as firewall configuration and access control policies.	Security controls are in place but there could be room for enhancement.
82	Are there formal processes in place for controlling and managing changes to the organization's systems and applications?	Evidence evidence of the formal processes in place for controlling and managing changes to the organization's systems and applications, such as change management policies and procedures.	Formal change management processes exist but they might not be fully optimized.
83	Are there processes in place for reviewing and approving configuration changes?	Evidence evidence of the processes in place for reviewing and approving configuration changes, such as change control boards and approval workflows.	Review and approval processes are in place but they may not be comprehensive.
84	Are there processes in place for testing and validating configuration changes before they are implemented in production?	Evidence evidence of the processes in place for testing and validating configuration changes before they are implemented in production, such as testing protocols and documented validation procedures.	Testing and validation are performed but there could be gaps.
85	Are there processes in place for documenting and tracking configuration changes?	Evidence evidence of the processes in place for documenting and tracking configuration changes, such as	Documentation and tracking are in place but there might be room for improvement.

		change request forms and documentation.	
86	Are there regular reviews of the configuration change process to ensure that it is operating effectively and that changes are being properly controlled?	Evidence evidence of the regular reviews of the configuration change process to ensure that it is operating effectively and that changes are being properly controlled, such as change management review reports.	Reviews are conducted but they may not be exhaustive.
87	Are there controls in place to ensure that the changes made by authorized personnel and are not made by unauthorized or malicious actors?	Evidence evidence of the controls in place to ensure that the changes made by authorized personnel and not made by unauthorized or malicious actors, such as access control policies and audit logs.	Controls exist but they might not catch all unauthorized activity.
88	Are there processes in place to rollback or undo any changes made in case of issues or problems detected after the change is implemented?	Evidence evidence of the processes in place to rollback or undo any changes made in case of issues or problems detected after the change is implemented, such as documented rollback procedures and change management policies.	Rollback processes are in place but they may not be foolproof.
89	Are there processes in place for regularly backing up the organization's information?	Evidence evidence of the processes in place for regularly backing up the organization's information, such as backup and recovery policies and procedures.	Backup processes are in place but there could be room for enhancement.
90	Are backups of the organization's information conducted on a regular schedule?	Evidence evidence of the backups of the organization's information conducted on a regular schedule, such as backup schedules and documentation.	Regular backups are conducted but the schedule might need adjustment.

91	Are the backups protected against unauthorized access, tampering or destruction?	Evidence evidence of the backups protected against unauthorized access, tampering, or destruction, such as access control policies and backup storage security controls.	Backups are protected but there could be gaps in security.
92	Are there processes in place for testing the recoverability of backups?	Evidence evidence of the processes in place for testing the recoverability of backups, such as documented backup testing protocols and procedures.	Backup recoverability tests are performed but they might not cover all scenarios.
93	Are there processes in place to ensure that backups are stored in a secure and offsite location?	Evidence evidence of the processes in place to ensure that backups are stored in a secure and offsite location, such as backup storage security controls and documentation.	Secure and offsite storage is used but there may be room for improvement.
94	Are there processes in place for restoring data from backups in case of data loss or disaster?	Evidence evidence of the processes in place for restoring data from backups in case of data loss or disaster, such as documented disaster recovery procedures and backup recovery protocols.	Data restoration processes exist but they could be refined.
95	Are the backup retention policies in place and aligned with the legal and regulatory requirements?	Evidence evidence of the backup retention policies in place and aligned with the legal and regulatory requirements, such as backup retention policies and documentation.	Backup retention policies are aligned but there could be room for improvement.
96	Are there regular tests of the backup process to ensure that it can be restored in case of an incident?	Evidence evidence of the regular tests of the backup process to ensure that it can be restored in case of an incident, such as documented backup testing protocols and procedures.	Backup tests are conducted but they might not cover all restoration scenarios.
97	Does the organization have documented Service Level Agreements (SLAs) for	Evidence evidence of documented Service Level Agreements (SLAs) for response and notification times	SLAs are documented but they might need updating or refinement.

	response and notification times for availability and security events?	for availability and security events, such as SLA policies and procedures.	
98	Are the SLAs for response and notification times for availability and security events communicated to all relevant parties, including external customers and partners?	Evidence evidence of the SLAs for response and notification times for availability and security events communicated to all relevant parties, such as customer and partner agreements and communication records.	SLAs are communicated but there may be some parties that are not fully informed.
99	Are there regular reviews of the SLAs for response and notification times for availability and security events to ensure they are still appropriate and effective?	Evidence evidence of the regular reviews of the SLAs for response and notification times for availability and security events to ensure they are still appropriate and effective, such as SLA review reports and documentation.	SLA reviews are performed but there could be gaps in the process.
100	Are there processes in place to measure and report on the organization's compliance with the SLAs for response and notification times for availability and security events?	Evidence evidence of the processes in place to measure and report on the organization's compliance with the SLAs for response and notification times for availability and security events, such as compliance reporting procedures and documentation.	Measurement and reporting processes are in place but they may not be exhaustive.
101	Are there contingencies in place in the event that the SLAs for response and notification times for availability and security events are not met?	Evidence evidence of the contingencies in place in the event that the SLAs for response and notification times for availability and security events are not met, such as incident response plans and escalation procedures.	Contingencies exist but there might be room for improvement.
102	Does the organization have a documented vendor risk assessment process in place?	Evidence evidence of the documented vendor risk assessment process in place, such as vendor risk	A vendor risk assessment process is documented but it could be refined.

		assessment policies and procedures.	
103	Are there processes in place for regularly reviewing and assessing the security controls of vendors and third-party service providers used by the organization?	Evidence evidence of the processes in place for regularly reviewing and assessing the security controls of vendors and thirdparty service providers used by the organization, such as vendor security assessment reports and documentation.	Security control assessments are conducted but there could be gaps in coverage.
104	Are there procedures for monitoring vendor compliance with the organization's security policies and standards?	Evidence evidence of the procedures for monitoring vendor compliance with the organization's security policies and standards, such as vendor compliance monitoring procedures and documentation.	Vendor compliance monitoring is in place but there might be room for enhancement.
105	Are there procedures for regularly reviewing and updating the list of approved vendors and third-party service providers used by the organization?	Evidence evidence of the procedures for regularly reviewing and updating the list of approved vendors and thirdparty service providers used by the organization, such as vendor management policies and procedures.	Vendor lists are reviewed but there could be room for improvement in the process.
106	Are there processes in place for addressing and mitigating risks associated with vendors and third-party service providers that do not meet the organization's security standards?	Evidence evidence of the processes in place for addressing and mitigating risks associated with vendors and thirdparty service providers that do not meet the organization's security standards, such as vendor risk mitigation procedures and documentation.	Risk mitigation processes are in place but they may not be fully effective.

107	Does the organization have a documented policy for determining, documenting, implementing and reviewing audit/log records?	Evidence evidence of the documented policy for determining, documenting, implementing, and reviewing audit/log records, such as audit policy and procedures.	An audit/log record policy is documented but it might need updating.
108	Are all systems, applications, and network devices configured to generate audit/log records?	Evidence evidence of all systems, applications, and network devices configured to generate audit/log records, such as system configuration documentation and audit log reports.	Audit/log record generation is configured but there might be gaps.
109	Are audit/log records regularly reviewed and analyzed to detect security incidents and anomalies?	Evidence evidence of audit/log records regularly reviewed and analyzed to detect security incidents and anomalies, such as audit log analysis reports and documentation.	Audit/log record review and analysis are performed but there could be blind spots.
110	Are there processes in place to ensure the integrity and confidentiality of audit/log records?	Evidence evidence of the processes in place to ensure the integrity and confidentiality of audit/log records, such as audit log storage and access control policies.	Integrity and confidentiality processes are in place but they may not be comprehensive.
111	Are there processes in place for preserving and retaining audit/log records for a specified period of time in accordance with the regulatory requirements?	Evidence evidence of the processes in place for preserving and retaining audit/log records for a specified period of time in accordance with regulatory requirements, such as audit log retention policies and documentation.	Preservation and retention processes exist but there might be room for improvement.
112	Is an antivirus or EDR/XDR solution currently in use within the organization?	Evidence evidence of an antivirus or EDR/XDR solution currently in use within the organization, such as antivirus software and documentation.	Antivirus or EDR/XDR solutions are in use but their coverage may not be complete.

113	Are all devices connected to the organization's network protected by an antivirus or EDR/XDR solution?	Evidence evidence of all devices connected to the organization's network protected by an antivirus or EDR/XDR solution, such as system configuration and software documentation.	Devices are protected but there could be gaps in coverage.
114	Are updates and patches for the antivirus or EDR/XDR solution applied in a timely manner?	Evidence evidence of updates and patches for the antivirus or EDR/XDR solution applied in a timely manner, such as patch management policies and procedures.	Updates and patches are applied but there might be room for improvement in timeliness.
115	Are regular scans for malware and other malicious software performed using the antivirus or EDR/XDR solution?	Evidence evidence of regular scans for malware and other malicious software performed using the antivirus or EDR/XDR solution, such as scan reports and documentation.	Regular scans are performed but there could be gaps in detection.
116	Is there a process in place for responding to and remediating any malware or other malicious software detected by the antivirus or EDR/XDR solution?	Evidence evidence of the process in place for responding to and remediating any malware or other malicious software detected by the antivirus or EDR/XDR solution, such as incident response plans and procedures.	Response and remediation processes are in place but they might not be fully optimized.
117	Are any remote control services, such as RDP, directly exposed to the internet?	Evidence evidence to confirm that remote control services, such as RDP, are not directly exposed to the internet, such as firewall rules and network diagrams.	Remote control services might be exposed but efforts are made to minimize risks.
118	Is there a mechanism in place to limit or restrict access to remote control services from external sources?	Evidence evidence of mechanisms in place to limit or restrict access to remote control services from external sources, such as remote access policies and procedures.	Access limitations exist but there might be room for improvement.

119	Are any external IP addresses or ranges explicitly blocked from accessing the organization's remote control services?	Evidence evidence of external IP addresses or ranges explicitly blocked from accessing the organization's remote control services, such as firewall rules and network diagrams.	External IP blocks are in place but there could be gaps.
120	Are strong authentication mechanisms, such as multi-factor authentication, required for accessing remote control services from external sources?	Evidence evidence of strong authentication mechanisms, such as multifactor authentication, required for accessing remote control services from external sources, such as remote access policies and procedures.	Strong authentication mechanisms are required but they might not cover all services.
121	Are there any monitoring or logging mechanisms in place to track and audit external access to remote control services?	Evidence evidence of monitoring or logging mechanisms in place to track and audit external access to remote control services, such as access logs and audit reports.	Monitoring and logging mechanisms are in place but there may be areas that are overlooked.
122	Are the organization's critically sensitive documents protected by encryption?	Evidence evidence that the organization's critically sensitive documents are protected by encryption, such as encryption policies and procedures.	Sensitive documents are encrypted but there might be room for enhancement.
123	Are the encryption methods used for protecting sensitive documents considered secure and up-to-date?	Evidence evidence that the encryption methods used for protecting sensitive documents are considered secure and up-to-date, such as encryption standards and encryption algorithms.	Encryption methods are secure but there could be room for improvement.
124	Are the encryption keys and other encryption-related information stored in a secure manner?	Evidence evidence that the encryption keys and other encryption-related information are stored in a secure manner, such as key management policies and procedures.	Encryption keys and information are stored securely but there might be areas for enhancement.

125	Are there any regular reviews or assessments of the encryption methods used to protect sensitive documents?	Evidence evidence of regular reviews or assessments of the encryption methods used to protect sensitive documents, such as encryption review reports and documentation.	Regular reviews or assessments of encryption methods are conducted but there may be room for improvement.
126	Are there any controls in place to ensure that only authorized personnel can access and decrypt the critically sensitive documents?	Evidence evidence of controls in place to ensure that only authorized personnel can access and decrypt the critically sensitive documents, such as access control policies and procedures.	Controls for document access and decryption are in place but they might not be comprehensive.
127	Is there a designated person or team within the organization responsible for cyber security?	Evidence evidence of a designated person or team within the organization responsible for cyber security, such as organizational charts and job descriptions.	A designated person or team exists for cyber security but their role might not be well-defined.
128	Is the person or team responsible for cyber security clearly defined and their roles and responsibilities understood throughout the organization?	Evidence evidence that the person or team responsible for cyber security is clearly defined, and their roles and responsibilities are understood throughout the organization, such as job descriptions and training records.	The cyber security team's roles and responsibilities are understood but there could be gaps in communication.
129	Does the person or team responsible for cyber security have the necessary knowledge, skills and experience to fulfill their role?	Evidence evidence that the person or team responsible for cyber security has the necessary knowledge, skills, and experience to fulfill their role, such as certifications and training records.	The cyber security team possesses necessary skills but there might be areas where additional training is needed.
130	Are the person or team responsible for cyber security have the appropriate level of access and authority to carry out their	Evidence evidence that the person or team responsible for cyber security has the appropriate level of access and authority to carry out their	The cyber security team has access and authority but there could be limitations in their effectiveness.

	responsibilities effectively?	responsibilities effectively, such as access control policies and procedures.	
131	Are the person or team responsible for cyber security reporting to appropriate level of management and are they held accountable for ensuring the security of the organization?	Evidence evidence that the person or team responsible for cyber security is reporting to appropriate levels of management and is held accountable for ensuring the security of the organization, such as performance review records and incident response reports.	The cyber security team reports to management and is held accountable but there might be room for improvement.
132	Are firewalls, proxies, and other network controls in place for detection and protection?	Evidence evidence that firewalls, proxies, and other network controls are in place for detection and protection, such as network diagrams and device configuration records.	Network controls such as firewalls and proxies are in place but they might not cover all possible threats.
133	Are the network controls configured properly and regularly maintained?	Evidence evidence that the network controls are configured properly and regularly maintained, such as change management records and device configuration reports.	Network controls are configured and maintained but there could be room for enhancement.
134	Are the network controls being used to enforce the organization's security policies and standards?	Evidence evidence that the network controls are being used to enforce the organization's security policies and standards, such as security policy documentation and access control policies and procedures.	Network controls enforce security policies but there might be gaps in their effectiveness.
135	Are logging mechanisms enabled for the network controls?	Evidence evidence that logging mechanisms are enabled for the network controls, such as device configuration	Logging mechanisms for network controls are enabled but there could be areas for improvement.

		records and access logs.	
136	Are the logs from the network controls being regularly reviewed, analyzed and retained for a sufficient period of time?	Evidence evidence that the logs from the network controls are regularly reviewed, analyzed, and retained for a sufficient period of time, such as log management policies and procedures and audit reports.	Logs from network controls are reviewed and retained but there might be room for enhancement in the process.



APPENDIX C

C.1 Sample of Persona-Based Assessment Kit

Organizational Chart					
Personas	P ₁	P ₂	P ₃	...	P _n
Titles of Personas					
Reporting to					
Organizational Objectives					
Value of Zero Trust					
Control Questions (Yes/No/Not Applicable)					
PB-CR1					
PB-CR2					
...					
PB-CRn					
Assessment					
Number of Audit Questions (naq)					
Number of Yes Answers (nya)					
Persona-Based Score (PBS)					
Assessment Result					

C.2 Ability Control Questions with their IDs for the Persona-Based Assessment Kit

- PB-CR.1 Does the organization ensure the security of other personas and other assets in the organization when this persona accesses to the specific resource of the organization remotely? (Without being physically inside the institution building.)
- PB-CR.2 Is the utilization of a virtual private network a prerequisite for accessing the organization's internal resources while external to the organization's physical location? Furthermore, if such utilization is mandated, is the enforcement of multi-factor authentication implemented as a requirement for gaining access via the virtual private network?
- PB-CR.3 Are there different levels of trust assigned to this persona?
- PB-CR.4 Are there corporate policies and procedures in place to verify the identity of this persona?
- PB-CR.5 Is there a comprehensive inventory of the assets this persona is associated with?
- PB-CR.6 Are there least privilege access controls in place or for this persona? Or, for this persona-specific, is there restricted to only the resources they need to perform their duty/job/operation?
- PB-CR.7 Are there procedures for removing access if an individual in the organization using a title for this persona leaves/transfers/replaces the organization?
- PB-CR.8 Are there protocols, policies and procedures in place for monitoring and login/logout events by this persona?
- PB-CR.9 Are there protocols in place for this persona, monitoring the failed logging access attempts from external sources?
- PB-CR.10 Is there a process in place for regularly reviewing and updating recovery plans for this persona?
- PB-CR.11 Is there a process in place for regularly reviewing and updating access controls for this persona?
- PB-CR.12 Does the organization ensure that this persona is aware of and trained on cyber security awareness regarding to zero trust and cyber resilience?
- PB-CR.13 Does the organization ensure that this persona is able to detect and report phishing attempts and other social engineering tactics?
- PB-CR.14 Are there procedures in place for verifying the identity of (internal/external) personas?
- PB-CR.15 Are there procedures in place for performing security risk assessments for (internal/external) personas?
- PB-CR.16 Are there procedures in place for performing daily/weekly self-compliance audits regarding to assess the compliance for NIST CSF, PCI DSS, and NIST SP 800-53 for this persona?
- PB-CR.17 Is there a process in place for regularly reviewing and updating security and compliance policies and procedures for this persona?

- PB-CR.18 An Active Directory security group has been used to identify authorized users and the corresponding persona is a member of a specific AD group.
- PB-CR.19 There is a SoD matrix for the AD group persona is in, and the related persona is subject to the SoD rules.
- PB-CR.20 Does centralized management solutions, such as Active Directory, enforce that the persona update their password on a periodic basis, and does this persona receives notifications and reminders about not using the same credentials in different applications?
- PB-CR.21 Are there any exceptions or deviations from the Zero Trust network architecture for this persona and if so, are they documented and justified?
- PB-CR.22 Are there procedures in place for performing penetration testing for this persona?
- PB-CR.23 The relevant persona does not have the authority to take policy exception action.
- PB-CR.24 The OS level user persona does not have local administrator rights. (End User Support persona is not subject to this question, they should be excluded.)
- PB-CR.25 The OS level user persona does not have domain administrator rights. (The IT Practitioner persona is not subject to this question, they should be excluded.)
- PB-CR.26 Does the related persona cannot login to their personal accounts due to some DLP policies through the digital inventory provided by the organization?
- PB-CR.27 Is multi-factor authentication required for all access attempts made by this person, with a maximum frequency of 1 week, at least monthly?

C.3 Ability Control Questions' References

PB-CR.1

ISO 27001:2013:

- A.9.2.2 - Secure remote access
- A.9.2.3 - Remote access policy
- A.9.2.4 - Remote access authentication
- A.9.2.5 - Remote access control
- A.9.2.6 - Remote access monitoring

NIST SP 800-53:

- AC-10 - Remote access enforcement
- AC-11 - Remote session termination
- AC-17 - Mobile code
- AC-19 - Remote access through VPN
- AC-20 - Remote access through wireless
- AC-22 - Remote access authentication

COBIT 5:

- IT-05 - IT management of third-party services
- IT-06 - IT governance of IT service continuity
- IT-07 - IT governance of IT service delivery and support
- IT-08 - IT governance of IT service level management

PCI DSS:

- Requirement 1 - Install and maintain a firewall configuration to protect cardholder data
- Requirement 7 - Restrict access to cardholder data by business need-to-know
- Requirement 8 - Assign a unique ID to each person with computer access
- Requirement 9 - Restrict physical access to cardholder data

HIPAA:

- 164.312(e)(1) - Remote use of workstations
- 164.312(e)(2) - Access control and validation procedures
- 164.312(e)(3) - Transmission security

SOC 2:

- Security - Common Criteria (CC) - Access controls
- Security - CC - Cryptographic controls
- Security - CC - Network security

Security - CC - Security management processes
Security - CC - System and communications protection

PB-CR.2

ISO 27001:2013:

A.9.2.4 - Remote access authentication
A.9.2.5 - Remote access control
A.9.2.6 - Remote access monitoring

COBIT 5:

IT-05 - IT management of third-party services
IT-08 - IT governance of IT service level management
IT-09 - IT governance of IT service quality

NIST SP 800-53:

AC-19 - Remote access through VPN
AC-22 - Remote access authentication
IA-2(2) - Multi-factor authentication

PCI DSS:

Requirement 1 - Install and maintain a firewall configuration to protect cardholder data
Requirement 8 - Assign a unique ID to each person with computer access
Requirement 9 - Restrict physical access to cardholder data

SOC 2:

Security - Common Criteria (CC) - Access controls
Security - CC - Cryptographic controls
Security - CC - Network security
Security - CC - Security management processes
Security - CC - System and communications protection

PB-CR.3

ISO 27001:2013:

A.9.1.1 - Access control policy
A.9.1.2 - Access control procedures
A.9.1.3 - Access control system management
A.9.1.4 - Access control system monitoring
A.9.1.5 - Access control system testing

NIST SP 800-53:

AC-2 - Identification and authentication policy and procedures
AC-3 - Session lock
AC-4 - Session termination
AC-6 - Authentication mechanisms
AC-7 - Authentication for non-network logon
AC-8 - Identification and authentication for network access

COBIT 5:

IT-05 - IT management of third-party services
IT-06 - IT governance of IT service continuity
IT-07 - IT governance of IT service delivery and support
IT-08 - IT governance of IT service level management

PB-CR.4

ISO 27001:2013:

A.9.2.4 - Remote access authentication
A.9.2.5 - Remote access control
A.9.2.6 - Remote access monitoring

NIST SP 800-53:

AC-2 - Identification and authentication policy and procedures
AC-3 - Session lock
AC-4 - Session termination
AC-6 - Authentication mechanisms
AC-7 - Authentication for non-network logon
AC-8 - Identification and authentication for network access

COBIT 5:

IT-05 - IT management of third-party services
IT-08 - IT governance of IT service level management
IT-09 - IT governance of IT service quality

SOC 2:

Security - Common Criteria (CC) - Access controls
Security - CC - Cryptographic controls
Security - CC - Network security

PB-CR.5

ISO 27001:2013:

A.12.1.1 - Asset classification and control
A.12.1.2 - Asset ownership
A.12.1.3 - Inventory of assets
A.12.2.2 - Operational procedures and responsibilities

NIST SP 800-53:

CM-3 - Configuration management policy and procedures
CM-4 - Configuration identification
CM-5 - Configuration control
CM-6 - Configuration status accounting
CM-7 - Configuration verification and auditing

COBIT 5:

IT-05 - IT management of third-party services
IT-06 - IT governance of IT service continuity
IT-07 - IT governance of IT service delivery and support
IT-08 - IT governance of IT service level management

SOC 2:

Security - Common Criteria (CC) - Access controls
Security - CC - Cryptographic controls
Security - CC - Network security
Security - CC - Security management processes

PB-CR.6

ISO 27001:2013:

A.9.1.1 - Access control policy
A.9.1.2 - Access control procedures
A.9.1.3 - Access control system management
A.9.1.4 - Access control system monitoring
A.9.1.5 - Access control system testing

NIST SP 800-53:

AC-2 - Identification and authentication policy and procedures
AC-3 - Session lock
AC-4 - Session termination
AC-6 - Authentication mechanisms
AC-7 - Authentication for non-network logon
AC-8 - Identification and authentication for network access
AC-17 - Least privilege
AC-18 - Role-based access control

COBIT 5:

IT-05 - IT management of third-party services
IT-08 - IT governance of IT service level management
IT-09 - IT governance of IT service quality

PB-CR.7

ISO 27001: A.9.2.4 Access control and management
NIST SP 800-53: AC-6 Access control
COBIT 5: APO12.08 Manage Access Authorizations
SOC 2: Trust Services Criteria - Security principle
HIPAA: The Security Rule (45 CFR 164.308(a)(4))- Termination of access.

PB-CR.8

ISO 27001: A.12.2.2 Logging and monitoring
NIST SP 800-53: SI-10 Audit and Accountability
COBIT 5: PO9.3 Monitor and Evaluate Security
SOC 2: Trust Services Criteria - Security principle
HIPAA: The Security Rule (45 CFR 164.312(b))- Monitoring and Logging
PCI DSS: Requirement 10.2 Review logs for all system components
NIST SP 1800-35: Section 3.2.1 Auditing and Accountability

PB-CR.9

ISO 27001 - Information Security Management Systems (ISMS):

A.12.2.2 Logging and monitoring
A.12.2.4 Information security incident management

NIST SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations:

SI-10 Audit and Accountability
SA-15 Account Monitoring
SI-7 Access Control

COBIT 5 - IT Governance Framework:

PO9.3 Monitor and Evaluate Security
PO9.2 Monitor and Evaluate Compliance

SOC 2 - Service Organization Control 2 - Trust Services Criteria:

Security principle
Availability principle

HIPAA - Health Insurance Portability and Accountability Act:

The Security Rule (45 CFR 164.312(b))- Monitoring and Logging

PCI DSS - Payment Card Industry Data Security Standard:

Requirement 10.2 Review logs for all system components

Requirement 10.5 Implement automated audit trails for all system components

NIST SP 1800-35 - Guide to Identifying an Information System as a National Security System:

Section 3.2.1 Auditing and Accountability - states that organizations must implement auditing and accountability mechanisms to monitor and log system access and activity, including failed login attempts from external sources.

PB-CR.10

ISO 22301 - Business Continuity Management Systems:

Clause 5.4.2 Business continuity planning

Clause 6.2.2 Evaluating and testing the BCMS

NIST SP 800-34 - Contingency Planning Guide for Federal Information Systems:

Section 4.3 Developing a Contingency Plan

Section 4.5 Testing and Exercising the Contingency Plan

COBIT 5 - IT Governance Framework:

PO10.2 Develop and Maintain Business Continuity Plans

PO10.3 Test and Exercise Business Continuity Plans

SOC 2 - Service Organization Control 2 - Trust Services Criteria:

Availability principle - requires an organization to establish and implement procedures to respond to an interruption of service

HIPAA - Health Insurance Portability and Accountability Act:

The Security Rule (45 CFR 164.308(a)(7)) - Contingency planning - requires a covered entity to implement procedures to restore any loss of data.

PCI DSS - Payment Card Industry Data Security Standard:

Requirement 12.9 Implement incident response plan, which includes procedures for responding to an incident and restoring normal system operations as quickly as possible, including employee-specific recovery plans.

NIST SP 1800-4 - Contingency Planning Guide for Federal Information Systems:

section 4.3 Developing a Contingency Plan

section 4.5 Testing and Exercising the Contingency Plan

PB-CR.11

ISO 27001 - Information Security Management Systems (ISMS):

A.9.2.1 Access control policy

A.9.2.2 Access control procedures

A.9.2.3 Access control rules

A.9.2.4 Access control responsibilities

A.9.2.5 Access control review

NIST SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations:

AC-2 Access Control Policy and Procedures

AC-3 Access Enforcement

AC-6 Maintenance of Access Control

COBIT 5 - IT Governance Framework:

PO7.1 Define and Manage Access Rights

PO7.2 Manage User Access

PO7.3 Review and Audit Access

SOC 2 - Service Organization Control 2 - Trust Services Criteria:

Security principle - requires an organization to establish and implement access controls to protect the confidentiality, integrity, and availability of the information.

HIPAA - Health Insurance Portability and Accountability Act:

The Security Rule (45 CFR 164.308(a)(4)) - Access controls - requires a covered entity to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs.

NIST SP 1800-35 - Guide to Identifying an Information System as a National Security System:

Section 3.3.1 Access Control - states that organizations must implement access controls to ensure that only authorized individuals are able to access national security systems and the data stored within them.

Section 3.3.1.1 Access Control Policy and Procedures - states that organizations must establish and implement a formal access control policy and procedures that are reviewed and updated regularly.

Section 3.3.1.2 Access Control Review and Maintenance - requires organizations to regularly review and update access controls to ensure they remain effective over time.

PB-CR.12

ISO 27001 - Information Security Management Systems (ISMS):

A.11.2.2 Information security awareness and training

NIST SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations:

SA-15 Information Security Awareness and Training

COBIT 5 - IT Governance Framework:

PO11.1 Manage IT Security Education and Awareness

SOC 2 - Service Organization Control 2 - Trust Services Criteria:

Security principle - requires an organization to develop and implement a security awareness and training program for personnel

NIST SP 1800-35 - Guide to Identifying an Information System as a National Security System:

Section 3.4.1.3 Information Security Training and Awareness - states that organizations must provide training and awareness programs that are designed to ensure that all personnel are aware of their roles and responsibilities with respect to information security.

NIST SP 800-137 - Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations:

Section 3.1 Cybersecurity-aware Culture - states that organizations should establish a cybersecurity-aware culture by providing training and awareness programs that instill a sense of shared responsibility for cybersecurity among all personnel.

PB-CR.13

ISO 27001 - Information Security Management Systems (ISMS):

A.11.2.2 Information security awareness and training

NIST SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations:

SA-15 Information Security Awareness and Training

PE-13 Incident Response and Management

COBIT 5 - IT Governance Framework:

PO11.1 Manage IT Security Education and Awareness

PO11.2 Identify and Respond to Security Incidents

SOC 2 - Service Organization Control 2 - Trust Services Criteria:

Security principle - requires an organization to develop and implement a security awareness and training program for personnel.

NIST SP 1800-35 - Guide to Identifying an Information System as a National Security System:

Section 3.4.1.3 Information Security Training and Awareness - states that organizations must provide training and awareness programs that are designed to ensure that all personnel are aware of their roles and responsibilities with respect to information security.

Section 3.4.1.4 Incident Response and Management - states that organizations must develop and implement incident response and management procedures that include procedures for detecting and reporting phishing attempts and other social engineering tactics.

PB-CR.14

ISO 27001 - Information Security Management Systems (ISMS):

A.9.2 Physical and environmental security

A.9.3 Communications and operations management

A.9.4 Access control

NIST SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations:

IA-2 Identification and Authentication (Organizational Users)

IA-2(1) Identification and Authentication Policy and Procedures

IA-2(2) Identification and Authentication Mechanisms

IA-2(3) Identification and Authentication of Organizational Users

COBIT 5 - IT Governance Framework:

PO11.2 Identify and Respond to Security Incidents

PO12.1 Manage Access Control

PO12.2 Manage Authentication

SOC 2 - Service Organization Control 2 - Trust Services Criteria:

Security principle - requires an organization to implement controls to verify the identity of individuals before granting access to systems and applications.

NIST SP 1800-35 - Guide to Identifying an Information System as a National Security System:

Section 3.3.1 Access Control - states that organizations must implement access controls to ensure that only authorized individuals are able to access national security systems and the data stored within them.

Section 3.3.1.1 Access Control Policy and Procedures - states that organizations must establish and implement a formal access control policy and procedures that are reviewed and updated regularly.

Section 3.3.1.2 Access Control Review and Maintenance - requires organizations.

PB-CR.15

NIST Cybersecurity Framework (CSF):

Identify and Protect: ID.RA-1, ID.RA-2, ID.RA-3

Detect: DE.RA-1, DE.RA-2, DE.RA-3

Respond: RS.RA-1, RS.RA-2, RS.RA-3

Recover: RC.RA-1, RC.RA-2, RC.RA-3

FISMA:

Security Management controls: FIPS 200

System and Services Acquisition: Special Publication 800-146

Security Assessment and Authorization: NIST SP 800-37

HIPAA:

Security Management Process: 164.308(a)(1)

Risk Analysis: 164.308(a)(1)(ii)(A)

Risk Management: 164.308(a)(1)(ii)(B)

FERPA:

Protecting Personally Identifiable Information: 34 CFR § 99.30

GLBA:

Information Security Program: § 501(b)

Risk Assessment: § 501(b)(2)

Incident Response: § 501(b)(2)"

SOX:

IT General Controls: § 302(a)

IT Application Controls: § 404(a)

ITIL:

IT Service Continuity Management: Service Continuity Management Process

IT Risk Management: ITIL Risk Management process

COBIT 2019:

Governance: PO10 - Governance of IT-related risks and opportunities

Management and Optimization: PO11 - Management and optimization of IT-related risks and opportunities

SOC 2:

Security: Trust Services Criteria (TSC) A.1

Availability: TSC A.2

Processing Integrity: TSC A.3

Confidentiality: TSC A.4

Privacy: TSC A.5

PCI DSS:

Requirement 12: Maintain a security policy: 12.1-12.2

Requirement 6: Develop and maintain secure systems and applications: 6.1-6.5

GDPR:

Article 32: Security of Processing: 32.1-32.2

Article 33: Notification of a personal data breach to the supervisory authority: 33.1-33.3

NIST SP 1800-35 "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)":

Risk Assessment: Section 2.3

CIS Critical Security Controls:

CSC 1: Inventory of Authorized and Unauthorized Devices: 1.1-1.2

CSC 2: Inventory of Authorized and Unauthorized Software: 2.1-2.2

CSA Cloud Control Matrix

Security Governance: CCM 01-04

Data Governance: CCM 05-09

Risk Management: CCM 10-13

ISO/IEC 27001:2013:

Clause 6: Planning: 6.1-6.3

Clause 8: Operation: 8.1-8.4

Clause 9: Performance Evaluation: 9.1-9.2

Clause 10: Improvement: 10.1-10.2

PB-CR.16

NIST Cybersecurity Framework (CSF):

Identify and Protect: ID.AM-1, ID.AM-2

Detect: DE.AM-1, DE.AM-2

Respond: RS.AM-1, RS.AM-2

Recover: RC.AM-1, RC.AM-2

SOX:

IT General Controls: § 302(a)

IT Application Controls: § 404(a)

ITIL:

IT Service Continuity Management: Service Continuity Management Process

IT Risk Management: ITIL Risk Management process

Compliance Management: ITIL Compliance Management process

COBIT 2019:

Governance: PO10 - Governance of IT-related risks and opportunities

Management and Optimization: PO11 - Management and optimization of IT-related risks and opportunities

Compliance: PO12 - Compliance with laws, regulations, standards and policies

SOC 2:

Security: Trust Services Criteria (TSC) A.1

Availability: TSC A.2

Processing Integrity: TSC A.3

Confidentiality: TSC A.4

Privacy: TSC A.5

PCI DSS:

Requirement 12: Maintain a security policy: 12.1-12.2

Requirement 6: Develop and maintain secure systems and applications: 6.1-6.5

Requirement 10: Track and monitor all access to network resources and cardholder data: 10.1-10.4

Requirement 11: Regularly test security systems and processes: 11.1-11.2"

GDPR:

Article 32: Security of Processing: 32.1-32.2

Article 33: Notification of a personal data breach to the supervisory authority: 33.1-33.3

Article 35: Data protection impact assessment: 35.1-35.2

Article 36: Prior consultation: 36.1

Article 37: Designation of the data protection officer: 37.1-37.3

NIST SP 1800-35 "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)":

Risk Assessment: Section 2.3

Compliance: Section 3.5

CIS Critical Security Controls:

CSC 1: Inventory of Authorized and Unauthorized Devices: 1.1-1.2

CSC 2: Inventory of Authorized and Unauthorized Software: 2.1-2.2

CSC 4: Continuous Vulnerability Management: 4.1-4.4

CSC 5: Controlled Use of Administrative Privileges: 5.1-5.3

PB-CR.17

NIST Cybersecurity Framework (CSF):

Identify and Protect: ID.AM-1, ID.AM-2

Detect: DE.AM-1, DE.AM-2

Respond: RS.AM-1, RS.AM-2

Recover: RC.AM-1, RC.AM-2

SOX:

IT General Controls: § 302(a)

IT Application Controls: § 404(a)

ITIL:

IT Service Continuity Management: Service Continuity Management Process

IT Risk Management: ITIL Risk Management process

Compliance Management: ITIL Compliance Management process

COBIT 2019:

Governance: PO10 - Governance of IT-related risks and opportunities

Management and Optimization: PO11 - Management and optimization of IT-related risks and opportunities

Compliance: PO12 - Compliance with laws, regulations, standards and policies"

SOC 2:

Security: Trust Services Criteria (TSC) A.1

Availability: TSC A.2

Processing Integrity: TSC A.3

Confidentiality: TSC A.4

Privacy: TSC A.5

PCI DSS:

Requirement 12: Maintain a security policy: 12.1-12.2

Requirement 6: Develop and maintain secure systems and applications: 6.1-6.5

Requirement 10: Track and monitor all access to network resources and cardholder data: 10.1-10.4

Requirement 11: Regularly test security systems and processes: 11.1-11.2

GDPR -

Article 32: Security of Processing: 32.1-32.2

Article 33: Notification of a personal data breach to the supervisory authority: 33.1-33.3

Article 35: Data protection impact assessment: 35.1-35.2

Article 36: Prior consultation: 36.1

Article 37: Designation of the data protection officer: 37.1-37.3

NIST SP 1800-35 "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)":

Risk Assessment: Section 2.3

Compliance: Section 3.5

CIS Critical Security Controls:

CSC 1: Inventory of Authorized and Unauthorized Devices: 1.1-1.2

CSC 2: Inventory of Authorized and Unauthorized Software: 2.1-2.2

CSC 4: Continuous Vulnerability Management: 4.1-4.4

CSC 5: Controlled Use of Administrative Privileges: 5.1-5.3

PB-CR.18

SOX:

IT General Controls: § 302(a)

IT Application Controls: § 404(a)

ITIL:

IT Service Continuity Management: Service Continuity Management Process

IT Risk Management: ITIL Risk Management process

Compliance Management: ITIL Compliance Management process

COBIT 2019:

Governance: PO10 - Governance of IT-related risks and opportunities

Management and Optimization: PO11 - Management and optimization of IT-related risks and opportunities

Compliance: PO12 - Compliance with laws, regulations, standards and policies

SOC 2:

Security: Trust Services Criteria (TSC) A.1

Availability: TSC A.2

Processing Integrity: TSC A.3

Confidentiality: TSC A.4

Privacy: TSC A.5

PCI DSS:

Requirement 12: Maintain a security policy: 12.1-12.2

Requirement 7: Restrict access to cardholder data by business need-to-know: 7.1-7.3

Requirement 10: Track and monitor all access to network resources and cardholder data: 10.1-10.4

Requirement 11: Regularly test security systems and processes: 11.1-11.2

GDPR:

Article 32: Security of Processing: 32.1-32.2

Article 33: Notification of a personal data breach to the supervisory authority: 33.1-33.3

Article 35: Data protection impact assessment: 35.1-35.2

Article 36: Prior consultation: 36.1

Article 37: Designation of the data protection officer: 37.1-37.3

NIST SP 1800-35 "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)":

Risk Assessment: Section 2.3

Compliance: Section 3.5

CIS Critical Security Controls:

CSC 1: Inventory of Authorized and Unauthorized Devices: 1.1-1.2

CSC 2: Inventory of Authorized and Unauthorized Software: 2.1-2.2

CSC 4: Continuous Vulnerability Management: 4.

PB-CR.19

ITIL:

IT Service Continuity Management: Service Continuity Management Process

IT Risk Management: ITIL Risk Management process

Compliance Management: ITIL Compliance Management process

COBIT 2019:

Governance: PO10 - Governance of IT-related risks and opportunities

Management and Optimization: PO11 - Management and optimization of IT-related risks and opportunities

Compliance: PO12 - Compliance with laws, regulations, standards and policies

SOC 2:

Security: Trust Services Criteria (TSC) A.1

Availability: TSC A.2

Processing Integrity: TSC A.3

Confidentiality: TSC A.4

Privacy: TSC A.5

PCI DSS:

Requirement 12: Maintain a security policy: 12.1-12.2

Requirement 7: Restrict access to cardholder data by business need-to-know: 7.1-7.3

Requirement 10: Track and monitor all access to network resources and cardholder data: 10.1-10.4

Requirement 11: Regularly test security systems and processes: 11.1-11.2

GDPR:

Article 32: Security of Processing: 32.1-32.2

Article 33: Notification of a personal data breach to the supervisory authority: 33.1-33.3

Article 35: Data protection impact assessment: 35.1-35.2

Article 36: Prior consultation: 36.1

Article 37: Designation of the data protection officer: 37.1-37.3

NIST SP 1800-35 "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)":

Risk Assessment: Section 2.3

Compliance: Section 3.5

CIS Critical Security Controls:

CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers: 3.1-3.4
CSC 7: Least Privilege: 7.1-7

PB-CR.20

NIST SP 800-63B "Digital Identity Guidelines":

Authentication and Lifecycle Management: Section 5.1
Memorized Secrets: Section 5.1.1
Memorized Secret Verifiers: Section 5.1.2
Memorized Secret Verifiers: Section 5.1.3
Notification of Compromise: Section 5.3.3

NIST SP 800-53A "Recommended Security Controls for Federal Information Systems and Organizations":

Security Management: AC-2, AC-3, AC-6
Access Control: AC-2(2), AC-3(2), AC-6(6)

PCI DSS:

Requirement 8: Assign a unique ID to each person with computer access: 8.1-8.5
Requirement 7: Restrict access to cardholder data by business need-to-know: 7.1-7.3
Requirement 8: Track and monitor all access to network resources and cardholder data: 8.1-8.5

ITIL:

IT Service Continuity Management: Service Continuity Management Process
IT Risk Management: ITIL Risk Management process
Compliance Management: ITIL Compliance Management process

COBIT 2019:

Governance: PO10 - Governance of IT-related risks and opportunities
Management and Optimization: PO11 - Management and optimization of IT-related risks and opportunities
Compliance: PO12 - Compliance with laws, regulations, standards and policies

SOC 2:

Security: Trust Services Criteria (TSC) A.1
Availability: TSC A.2
Processing Integrity: TSC A.3
Confidentiality: TSC A.4
Privacy: TSC A.5

GDPR:

Article 32: Security of Processing: 32.1-32.2

Article 33: Notification of a personal data breach.

PB-CR.21

NIST Cybersecurity Framework (CSF):

Identify: ID.RA-2, ID.RA-3

Protect: PR.RA-1, PR.RA-2

Detect: DE.RA-1

Respond: RS.RA-2

Recover: RC.RA-1

NIST SP 800-39 "Managing Risk from Information Systems: An Organizational Perspective":

Section 3.1 "Risk Management Framework"

Section 3.2 "Risk Assessment"

Section 3.3 "Risk Response"

Section 3.4 "Risk Monitoring"

NIST SP 800-30 "Guide for Conducting Risk Assessments":

Section 2 "Risk Assessment Process"

Section 3 "Risk Assessment Methods"

Section 4 "Risk Assessment Report"

NIST SP 800-37 "Guide for Applying the Risk Management Framework to Federal Information Systems":

Section 2 "Risk Management Framework"

Section 3 "Risk Assessment"

Section 4 "Risk Response"

Section 5 "Risk Monitoring"

ISO 2700:

Clause 6.1

Clause 6.2

Clause 6.3

COBIT 2019:

Governance: PO10 - Governance of IT-related risks and opportunities

Management and Optimization: PO11 - Management and optimization of IT-related risks and opportunities

Compliance: PO12 - Compliance with laws, regulations, standards and policies

SOC 2:

Security: Trust Services Criteria (TSC) A.1

Availability: TSC A.2

Processing Integrity: TSC A.3

Confidentiality: TSC A.4

Privacy: TSC A.5

PCI DSS:

Requirement 12: Maintain a policy that addresses information security for all personnel:
12.1-12.6

Requirement 6: Develop and maintain secure systems and applications: 6.1-6.6

Requirement 8: Regularly monitor and test networks: 8.1-8.14

PB-CR.22

NIST Cybersecurity Framework (CSF):

Detect: DE.DP-2

Respond: RS.DP-1

NIST SP 800-115 "Technical Guide to Information Security Testing and Assessment"

Section 5 "Testing Methodologies"

Section 7 "Penetration Testing"

NIST SP 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations"

Control AC-17 "Penetration Testing"

ISO 27001:

Clause 9.2 "Security testing"

Clause 9.3 "Penetration testing"

COBIT 2019:

Management and Optimization: PO9 - Management and optimization of IT-related security

Compliance: PO12 - Compliance with laws, regulations, standards and policies

SOC 2:

Security: Trust Services Criteria (TSC) A.1

Availability: TSC A.2
Processing Integrity: TSC A.3
Confidentiality: TSC A.4
Privacy: TSC A.5

PCI DSS:

Requirement 11: Regularly test security systems and processes: 11.1-11.3

PB-CR.23

NIST Cybersecurity Framework (CSF):

Identify: ID.CM-1
Protect: PR.AC-2
Detect: DE.DP-2
Respond: RS.DP-1
Recover: RS.DP-1

NIST SP 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations"

Control AC-1 "Access Control Policy and Procedures"
Control AC-2 "Account Management"

ISO 27001:

Clause 5.1
Clause 6.1

COBIT 2019:

Management and Optimization: PO1 - Governance of IT
Compliance: PO12 - Compliance with laws, regulations, standards and policies

SOC 2:

Security: Trust Services Criteria (TSC) A.1
Availability: TSC A.2
Processing Integrity: TSC A.3
Confidentiality: TSC A.4
Privacy: TSC A.5

PCI DSS:

Requirement 12: Maintain a policy that addresses information security for all personnel

PB-CR.24

NIST Cybersecurity Framework (CSF):

Identify: ID.CM-1
Protect: PR.AC-3
Detect: DE.DP-2
Respond: RS.DP-1
Recover: RS.DP-1

NIST SP 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations"

Control AC-3 "Access Enforcement"
Control AC-6 "Least Privilege"
Control AC-16 "Separation of Duties"

ISO 27001:

Clause 6.2 "User access management"
Clause 6.3 "User responsibilities"

COBIT 2019:

Management and Optimization: PO1 - Governance of IT
Compliance: PO12 - Compliance with laws, regulations, standards and policies"

SOC 2:

Security: Trust Services Criteria (TSC) A.1
Availability: TSC A.2
Processing Integrity: TSC A.3
Confidentiality: TSC A.4
Privacy: TSC A.5

PCI DSS:

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.
Requirement 3: Protect stored cardholder data.

SOX:

IT General Controls: § 302(a)
IT Application Controls: § 404(a)

PB-CR.25

NIST Cybersecurity Framework (CSF):

Identify: ID.CM-1
Protect: PR.AC-3
Detect: DE.DP-2
Respond: RS.DP-1
Recover: RS.DP-1

NIST SP 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations":

Control AC-3 "Access Enforcement"
Control AC-6 "Least Privilege"
Control AC-16 "Separation of Duties"

ISO 27001:

Clause 6.2 "User access management"
Clause 6.3 "User responsibilities"

COBIT 2019:

Management and Optimization: PO1 - Governance of IT
Compliance: PO12 - Compliance with laws, regulations, standards and policies

SOC 2:

Security: Trust Services Criteria (TSC) A.1
Availability: TSC A.2
Processing Integrity: TSC A.3
Confidentiality: TSC A.4
Privacy: TSC A.5

PCI DSS:

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.
Requirement 3: Protect stored cardholder data.

PB-CR.26

NIST Cybersecurity Framework (CSF):

Identify: ID.AM-2
Protect: PR.DS-1, PR.DS-2
Detect: DE.CM-1
Respond: RS.CM-1
Recover: RS.CM-1

NIST SP 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations"

Control SI-4 "Information Flow Enforcement"

Control SC-13 "Data Loss Prevention"

ISO 27001:

Clause 8.2 "Information classification"

Clause 9.1 "Security incident management"

COBIT 2019:

Management and Optimization: PO1 - Governance of IT

Compliance: PO12 - Compliance with laws, regulations, standards and policies

SOC 2:

Security: Trust Services Criteria (TSC) A.1

Availability: TSC A.2

Processing Integrity: TSC A.3

Confidentiality: TSC A.4

Privacy: TSC A.5

PCI DSS:

Requirement 11: Regularly test security systems and processes.

Requirement 12: Maintain a policy that addresses information security for all personnel.

PB-CR.27

NIST Cybersecurity Framework (CSF):

Identify: ID.AM-3

Protect: PR.AC-3

Detect: DE.AE-2

NIST SP 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations"

Control IA-2(1) "Authenticator management"

Control IA-2(2) "Authenticator usage"

ISO 27001:

Clause 8.3 "Access control"

COBIT 2019:

Management and Optimization: PO2 - Risk Management

Governance of IT: PO3 - Performance Measurement

Compliance: PO12 - Compliance with laws, regulations, standards and policies

SOC 2:

Security: Trust Services Criteria (TSC) A.1

Availability: TSC A.2

Processing Integrity: TSC A.3

Confidentiality: TSC A.4

Privacy: TSC A.5"

PCI DSS:

Requirement 8: Use of multi-factor authentication

APPENDIX D

D.1 Sample Audit Report

PROPRIETARY AND CONFIDENTIAL

This report presents the results of Cyber Resiliency audits conducted for [Organization Name] to assess the organization's cyber resiliency. The audits focused on two key aspects: Persona-Based Cyber Resiliency and Risk-Based Cyber Resiliency. These audits were conducted to evaluate the effectiveness of the organization's cyber security measures and provide recommendations to improve its overall cyber resiliency.

Audit Results

Persona-Based Cyber Resiliency

This audit assessed the organization's ability to maintain essential personas in the face of cyber threats, considering the security controls operating at a granular level, roles, responsibilities, and awareness of employees, management, and other stakeholders. The audit evaluated training, incident response plans, and security awareness programs.

Persona-Based Cyber Resiliency Score: 25,64 (out of 100)

Risk-Based Cyber Resiliency Audit

This audit assessed the organization's ability to manage and mitigate cyber risks by evaluating the effectiveness of security controls, policies, and procedures. The audit covered data protection, network security, access control, and vendor risk management.

Risk-Based Cyber Resiliency Score: 50,34 (out of 100)

Total Score of Cyber Resiliency

Aspect	Score (out of 100)	Weightage	Weighted Score
Persona-Based Cyber Resiliency	25,64	30%	7,69
Risk-Based Cyber Resiliency	50,34	70%	35,23
Total Cyber Resiliency Score	42,92		

PROPRIETARY AND CONFIDENTIAL

Conclusion and Recommendations

Based on audit findings, the organization's current score of 42.92 out of 100 indicates that its cybersecurity posture has significant room for improvement. Numerous deficiencies were discovered during the audit, particularly in the areas of information security policy, access management, incident response, vulnerability management, data security, and legal and regulatory compliance.

In addition, the audit uncovered a lack of emphasis on human factors in cyber-resilience and limited scalability and adaptability of cyber-resilience strategies. These issues highlight the need for a holistic approach to cybersecurity, which includes not only technical measures but also organizational and behavioral aspects.

To address these gaps and reinforce the organization's cyber resilience, it is recommended to implement the following measures:

- **Policy Development and Review:** If an organization doesn't have a comprehensive and current information security policy, they should consider developing one. This policy should outline how the organization will safeguard sensitive data, including incident response, reporting procedures, and legal and regulatory compliance. This policy should be reviewed and updated frequently to ensure that it remains effective and up-to-date.
- **Training and Awareness:** As part of their onboarding or training, all employees and contractors should be required to evaluate and acknowledge the information security policy. Staff should be educated on the significance of data security and how to recognize and respond to potential cyber threats through regular training and awareness campaigns.
- **Compliance Monitoring and Enforcement:** The organization should have processes for enforcing its information security policy, such as regular audits and compliance monitoring. Responsible for assuring compliance with legal and regulatory requirements for cyber security should be designated individuals or teams.
- **Asset Management:** The organization should have a system for inventorying and monitoring all physical devices and systems, as well as for performing routine maintenance and updates. Devices that are no longer in use must have their data erased or obliterated before being discarded in a secure manner.

PROPRIETARY AND CONFIDENTIAL

- **Incident Response Planning:** The organization must have a documented incident response plan for coping with various cyber threats, including ransomware attacks. This plan should be routinely tested and revised.
- **Vulnerability Management:** A documented vulnerability management program should be in place at the organization, with identified vulnerabilities being effectively monitored and managed. Regular audits of the organization's inventory of assets should be performed to ensure that all assets are accounted for and that newly acquired assets are evaluated for vulnerabilities.
- **Access Control:** The organization should have formal mechanisms in place for provisioning and deprovisioning user access to systems and applications. Only those with a legitimate business need should be granted access, and automated procedures should be in place for revoking access for terminated employees or contractors.
- **Data Security:** Measures should be in place to protect data-at-rest, including encryption and access controls. Regular backups of sensitive data should be created and secured with encryption and other safeguards.
- **Environment Segregation:** To prevent unauthorized access and data leakage, the organization should have unambiguous separation and isolation between the development, testing, and production environments. Network and system records should be regularly monitored and audited to detect any unauthorized access or data leakage.
- **Change Management:** The organization should implement formal procedures for governing and managing system and application modifications. Changes to the configuration should be reviewed, approved, tested, and validated prior to implementation in production.
- **Vendor Risk Management:** The organization should have a documented vendor risk assessment process in place, with processes for regularly reviewing and assessing the security controls of vendors and third-party service providers.
- **Log Management:** The organization should have a documented policy for identifying, documenting, implementing, and evaluating audit/log records. Every system, application, and network device should be configured to produce audit/log records.
- **Designated Security Personnel:** The organization should have a designated person or team responsible for cyber security, with clearly defined roles and responsibilities. This individual or group must have the appropriate level of access and authority to effectively carry out their responsibilities.

PROPRIETARY AND CONFIDENTIAL

The organization can further enhance its cyber resilience and maintain a robust security posture against evolving cyber threats by addressing these identified areas. The cyber resiliency score scale can be observed below.

Score Range	Classification
90-100	Excellent
80-89	Very Good
70-79	Good
60-69	Satisfactory
50-59	Below Average
40-49	Poor
30-39	Very Poor
20-29	Extremely Poor
10-19	Critically Low Resiliency
0-9	Negligible Resiliency

Also, to address the identified gaps and enhance the overall security posture, the organization can consider adhering to the following information security standards and benchmarks:

ISO/IEC 27001:

- Section 5: Leadership: The organization's top management should establish its information security policy and ensure that it is aligned with its business objectives. They should also ensure that information security roles and responsibilities are explicitly defined.
- Section 6: Planning: The organization must conduct risk assessments and use the results to establish information security objectives.
- Section 7: Support: This section addresses awareness and training, which could remedy the lack of employee understanding of the organization's security policies and procedures.
- Operation: This includes conducting risk assessments and managing changes, which could assist the organization in enhancing its vulnerability management program.

PROPRIETARY AND CONFIDENTIAL

The NIST Cybersecurity Framework:

- **Determine:** Acquire the knowledge necessary to manage cybersecurity risk to systems, people, assets, data, and capabilities. This includes asset management, the business environment, governance, risk assessment, and the strategy for risk management.
- **Protect:** Develop and implement safeguards to assure the delivery of essential services. This includes access control, information security, awareness and training, and protective technology.
- **Respond:** Develop and implement the appropriate activities to address a detected cybersecurity incident. This consists of response planning, communication, analysis, mitigation, and enhancements.

CIS Controls:

- **CIS Control 1: Inventory and Control of Hardware Assets:** Could aid in resolving problems with device tracking and maintenance.
- **CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers:** May assist in enhancing the organization's change management processes.
- **CIS Control 18: Application Software Security:** May assist with vendor risk management issues.

COBIT:

- **BAI03: Manage Configuration:** Might assist in enhancing the organization's change management processes.
- **DSS05: Manage Security Services:** May assist the organization in enhancing its incident response and reporting processes.

PCI DSS:

- **Maintain a Policy Regarding Information Security for All Employees:** This stipulation could assist the organization in enhancing its information security policy and employee awareness. This requirement may assist the organization in enhancing its vulnerability management program.

PROPRIETARY AND CONFIDENTIAL

SOC 2:

- Security: Both physical and logical unauthorized access to the system is prevented.
- Availability: The system is available for operation and use in accordance with the commitments or agreements.
- Confidentiality: Identified confidential information is safeguarded.

GDPR:

- Article 32: Processing Security: This could assist the organization in enhancing its data protection measures.

Article 33: Notification of a Personal Data Breach to the Supervisory Authority: This could help the organization enhance its incident response and reporting procedures.

CURRICULUM VITAE

Personal Information

Name and surname: Yaprak Kurtlutepe

Academic Background

Bachelor's Degree Education: Management Information Systems, Kadir Has University, Istanbul, Turkey

Foreign Languages: French, English

Work Experience

Institutions Served and Their Dates:

Coca-Cola İçecek, June, 2021 - Present

Kadir Has University Center For Cybersecurity and Critical Infrastructure Protection,
August 2018, June 2021