ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL

ANALYSIS OF INFORMATION SECURITY FRAMEWORKS FOR SMALL AND MEDIUM-SIZED ENTERPRISES (SMEs): INVESTIGATION OF ATTACKS AND MITIGATION PROPOSALS

M.Sc. THESIS

Gizemnur TAŞKIN

Department of Computer Engineering

Computer Engineering Programme

FEBRUARY 2024

ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL

ANALYSIS OF INFORMATION SECURITY FRAMEWORKS FOR SMALL AND MEDIUM-SIZED ENTERPRISES (SMEs): INVESTIGATION OF ATTACKS AND MITIGATION PROPOSALS

M.Sc. THESIS

Gizemnur TAŞKIN
(504201523)

Department of Computer Engineering

Computer Engineering Programme

Thesis Advisor: Asst. Prof. Dr. Mehmet Tahir SANDIKKAYA

FEBRUARY 2024

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

KOBİ'LER İÇİN BİLGİ GÜVENLİĞİ ÇERÇEVELERİNİN ANALİZİ, SALDIRILARIN İNCELENMESİ VE ÇÖZÜM ÖNERİLERİ

YÜKSEK LİSANS TEZİ

Gizemnur TAŞKIN
(504201523)

Bilgisayar Mühendisliği Anabilim Dalı

Bilisayar Mühendisliği Programı

Tez Danışmanı: Asst. Prof. Dr. Mehmet Tahir SANDIKKAYA

ŞUBAT 2024

Gizemnur TAŞKIN, a M.Sc. student of ITU Graduate School student ID 504201523 successfully defended the thesis entitled "ANALYSIS OF INFORMATION SECURITY FRAMEWORKS FOR SMALL AND MEDIUM-SIZED ENTERPRISES (SMEs): INVESTIGATION OF ATTACKS AND MITIGATION PROPOSALS", which she prepared after fulfilling the requirements specified in the associated legislations, before the jury whose signatures are below.

Thesis Advisor :	**Asst. Prof. Dr. Mehmet Tahir SANDIKKAYA** Istanbul Technical University	.....
Jury Members :	**Asst. Prof. Dr. Barış CELİKTAS** Işık University	.....
	Assoc. Prof. Dr.Ahmet Cüneyd TANTUG Istanbul Technical University	.....

Date of Submission : **05 January 2024**
Date of Defense : **14 February 2024**

To my family,

FOREWORD

First of all, I would like to express my gratitude to my advisor Asst. Prof. Dr. Mehmet Tahir SANDIKKAYA for his valuable guidance, support, and motivation throughout the completion process of this thesis. His strong support and encouragement played a significant role in overcoming the challenges I faced on my academic journey, contributing to the emergence of this thesis. Throughout my student life, I have learned many new things and had the opportunity to continuously improve myself. On this occasion, I would like to express one more gratitude to my esteemed advisor, who approached me not only as a student but also as an individual, providing constant opportunities for learning. The time spent under his guidance has been an unforgettable experience for me.

Additionally, I would like to extend my thanks to all the faculty members within Istanbul Technical University from whom I have taken courses thus far. Through their wealth of knowledge, passion for teaching, and dedicated efforts, I have had the opportunity to continuously enhance myself.

Finally, I express my gratitude to my dear family for their patience and unwavering support. This thesis has been shaped by all of your guidance, and I extend my thanks to everyone who has supported me along this journey.

February 2024 Gizemnur TAŞKIN

TABLE OF CONTENTS

ABBREVIATIONS

SMEs	: Small to Medium-sized Enterprises
ISO	: the International Organization for Standardization
NIST	: National Institute of Standards and Technology
NIST IR	: NIST Internal Report
TCA	: Turkish Court of Accounts
ICSG	: Information and Communication Security Guide
ICS audit	: Information and Communication Security audit
IT	: Information Technology
ISMS	: Information Security Management Systems
KVKK	: Personal Data Protection Law 6698 of Turkey
GDPR	: General Data Protection Regulation
CSF	: Cyber Security Framework
KAMI	: Information Security Index of Indonesia
SP	: special publication
NIST SP 800 Series	: privacy and security requirements in information systems
ISO/IEC 27000 Series	: security in information systems management
PCI DSS	: Payment Card Industry Data Security Standard
SSAE 16	: the Statement on Standards for Attestation Engagements No. 16
COBIT	: Control Objectives for Information and Related Technologies
ITIL	: Information Technology Infrastructure Library
BSI	: Federal Office for Information Security in Germany
IT-Grundschutz	: IT Baseline Protection Manual
ENISA	: The European Union Agency for Cybersecurity
SMECRA	: SME Cyber Risk Assessment
MESEs	: Micro and Small Enterprises
PDCA	: Plan-Do-Check-Act
INTOSAI	: International Organization of Supreme Audit Institutions
ISACA	: Information Systems Audit and Control Association
ISO/IEC 15408	: Information security, cybersecurity and privacy protection
ISO/IEC 38500	: Governance of IT for the organization
TOGAF	: The Open Group Architecture Framework
PMBOK	: Project Management Body of Knowledge
TSE	: Turkish Standards Institution
CIS	: Center for Internet Security
OWASP	: Open Web Application Security Project
CSF14	: Framework for Improving Critical Infrastructure Cybersecurity
IoT	: Internet of Things
PCER	: Plan, Control, Evaluate, and Report
IPDRR	: Identify, Protect, Detect, Respond, Recover
CD	: Compact Disc
DVD	: Digital Video Disc
PII	: Personally Identifiable Information

SYMBOLS

M	**:** Measure
F	**:** Frequency
$\mathbf{M_s}$	**:** Measure of scope s
W	**:** Weight
E	**:** Easiness

LIST OF TABLES

Page

LIST OF FIGURES

Page

ANALYSIS OF INFORMATION SECURITY FRAMEWORKS FOR SMALL AND MEDIUM-SIZED ENTERPRISES (SMEs): INVESTIGATION OF ATTACKS AND MITIGATION PROPOSALS

SUMMARY

Small and Medium-sized Enterprises (SMEs) are crucial on a global scale, constituting 90% of all businesses worldwide and providing 50% of employment. These figures are even higher in developing countries. With the increasing opportunities for online business, every enterprise is making technological advancements. However, the rate of cyber attacks is also rising dramatically. As a result, cybersecurity measures have become essential for businesses of all sizes. Larger and more developed enterprises are often resilient to such attacks due to the budget and time they allocate to cybersecurity, as well as the qualified professionals they employ. However, SMEs are more susceptible. Hence, over half of the attacks on businesses worldwide target SMEs.

While large enterprises benefit from well-established cybersecurity frameworks like ISO 27001, the need for information security management also arises for SMEs. Unfortunately, there is a limited number of informative articles or studies on information security specifically tailored to SMEs, unlike the abundant resources available for larger enterprises. This thesis aims to conduct a detailed analysis and comparison of security frameworks such as ISO 27001, NIST IR 7621, the Turkish Court of Accounts (TCA)'s IT audit, and the Communication Security Guide from the Presidency of the Republic of Turkey digital transformation office (ICSG), specifically focusing on the context of SMEs. ISO 27001 is a globally recognized security framework with certifications obtained by tens of thousands of businesses worldwide. Although NIST IR 7621 has been developed for small and medium-sized enterprises (SMEs), its methods and content are not widely represented in studies. On the other hand, TCA's IT audit and ICSG are structures that provide security solutions for businesses in Turkey, and there is a limited amount of research available on both. Each of these structures, with distinct focuses, offers various standards and guidelines for businesses in managing information security. The aforementioned frameworks, along with analyses of the attack types commonly encountered by SMEs, have been assessed, ranked, and presented. Furthermore, based on these analyses, cost-effective and easily implementable security measures have been proposed for SMEs. The effectiveness of these security measures in addressing evolving security issues has been evaluated.

KOBİ'LER İÇİN BİLGİ GÜVENLİĞİ ÇERÇEVELERİNİN ANALİZİ, SALDIRILARIN İNCELENMESİ VE ÇÖZÜM ÖNERİLERİ

ÖZET

Küçük ve orta ölçekli işletmelerin (KOBİ'lerin) günümüz iş dünyasında kritik rol taşır. Öyledir ki, Dünya Bankası dünya genelinde bütün işletmelerin %90'ını oluşturduklarını ve %50 oranında istihdam sağladıklarını belirtmektedir. Bu oran gelişmekte olan ülkeler için daha da fazladır. KOBİ'ler, ekonomik büyümenin temel taşları olarak iş dünyasında çeşitli sektörlerde faaliyet göstermekte ve geniş bir istihdam potansiyeli sunmaktadır. Teknolojinin hızlı gelişimi, çevrimiçi iş fırsatlarını geleneksel iş modellerinin ötesine taşımıştır. Böylece internetin yaygın kullanımı, işletmelerin küresel pazarlara erişimini kolaylaştırırken, çevrimiçi platformlar aracılığıyla yeni iş alanlarının kapılarını aralamıştır. Ancak, bu dijital dönüşüm, işletmeleri sadece fırsatlarla değil, aynı zamanda artan siber tehditlerle de karşı karşıya bırakır. Buna bağlı olarak, teknolojik ilerleme aynı zamanda siber saldırılar için yeni kapılar açar. İşletmelerin dijital varlıkları, hızla evrilen tehditlerle karşı karşıya kalmasına neden olur. Siber saldırılar işletmelerin bilgi sisteminin zarar görmesini, yasa düzenleyiciler tarafından cezalandırılmasını, işletme üretkenliğin azalmasını, kritik bilgilerin kaybından kaynaklanan iş sürdürülebilirliğinin azalmasını, itibar veya güven kaybı yaşamaları, kredi almalarının zorlaşmasını ve bankalardan kredi alamamalarını, veya işletme gelirinin kaybına neden olabilmektedir. Bu durum, işletmelerin bilgi güvenliği önlemlerini güçlendirmelerini zorunlu kılar. Büyük işletmeler, gerek ayırdıkları bütçe ile gerek yetenekli çalışan gücü ile bu önlemleri daha kolay alabilmektedir. Ancak, sınırlı finansal ve bilgi kaynaklarına sahip olmaları, KOBİ'lerin nitelikli çalışan veya danışman bulamamaları ve genellikle karmaşık bilgi güvenliği önlemleri ile karşılaşmaları bu işletmelerin sürdürülebilirliklerini ve büyümelerini tehlikeye atmaktadır. Yeterli güvenlik önlemleri alamayan KOBİ'ler, yapılan araştırmalarda dünya genelindeki tüm saldırıların yarısından fazlasa maruz kalmaktadır.

KOBİ'lerin güvenlik altyapılarını oluşturmak ve güçlendirmek, sadece iş sürekliliği ve müşteri güveni açısından değil, aynı zamanda genel ekonomik istikrar açısından da kritik bir öneme sahiptir. Ayrıca, KOBİ'lerin yasal zorunluluklara uyum sağlamaları da gerektiği durumlar yaşanmaktadır. Örneğin, Kişisel Verileri Koruma Kanunu (KVKK) gibi düzenlemelerle işletmelerin yasal olarak koruması gereken bilgiler bulunmaktadır. Böylece yasa düzenleyiciler tarafından denetlenmek zorunda kalan işletmeler için de bilgi güvenliğinin sağlanması zorunlu hale gelmiştir. Bu tez, bu önemli aktörlerin karşılaştığı güvenlik zorluklarını anlamak ve etkili bir güvenlik çerçevesi oluşturmak için yapılan analizleri içermektedir. ISO 27001, NIST IR 7621, Sayıştay Bilişim Teknolojileri Denetleme Raporu ve İletişim Bakanlığının Bilgi ve İletişim Güvenliği Rehberi gibi dört önemli bilgi güvenliği çerçevelerinin

incelenmesiyle başlayan çalışma, bu çerçevelerin özelliklerini ve avantajlarını ayrıntılı bir şekilde ele almaktadır. ISO 27001 on binlerce işletme tarafından sertifikası alınmış, en bilindik bilgi güvenliği sistemlerinden biridir. NIST IR, küçük işletmeler için ortaya çıkmış önerilerden oluşan teknik bilgiden uzak bir yapıdır. Sayıştay Bilişim Teknolojileri Denetleme Raporu ve Bilgi ve İletişim Güvenliği Rehberi ise, Türkiye Cumhuriyeti tarafından kamu kurum, kuruluş ve kritik bilgi taşıyan işletmeler için ortaya çıkmıştır. Fakat her iki belge de tüm işletmelerin de isteğe bağlı olarak kullanabileceği vurgulanmıştır. Türkiye tarafından yayınlanan bu iki belgenin de hala yürürlükte olması, ve iki belge hakkında yeterli kaynağın bulunmaması da analize eklenmelerinde büyük rol oynamıştır. Farklı karakteristik özelliklere sahip olan bu dört güvenlik yapısı; tanım, yapı, mekanizma, kapsam, iş akışı, belgelendirilebilir olması, zorunlu belgelere sahip olması, karmaşıklık, hedef organizasyon ve mevcudiyet açısından değerlendirilmiştir.

Bu değerlendirmenin sonucunda da bazı sonuçlar ortaya çıkmıştır. ISO 27001 ve Bilgi ve İletişim Güvenliği Rehberi belirtilen yapılar içerisinde en kapsamlı iki çerçevedir. ISO 27001'in sertifikalandırma özelliği kullanıcılara güven aşılamaktadır. Ayrıca, hedeflenen işletme türü boyutundan veya endüstrisinden bağımsızdır. Esnek yapısı ile her türden işletmeye uyum sağlayabilir. Dili teknik dilden uzaktır, fakat uygulanan işletmede bilgi teknolojisi gerekmektedir. Ek olarak, diğer üç yapıdan farklı olarak mevcudiyet açısından değerlendirildiğinde, erişimi daha zordur. ISO 27001 ücret karşılığında erişilebilir olmasıdan ve bir denetçi tarafından sertifikalandırıldığından maliyetli ve erişimi zor bir seçenektir.

Küçük işletmeler için hazırlanmış olan NIST IR 7621, 20 teknik olmayan öneri ile belirttiği kapsamları karşılamaktadır. Kapsam bakımından sınırlı olan bu belge, küçük işletmeler için maliyetsiz önlemler sunar. Kolay ulaşılabilir ve uygulanabilirdir.

Sayıştay Bilişim Teknolojileri Denetleme Raporu mali sorunları önlemek için kabul edilen, bilişim teknolojileri kullanımını ve güvenliğini değerlendirmek amacıyla kullanılan bir rehberdir. Devlet tarafından yönlendirilen denetçiler tarafından kullanılır. Bu yüzden teknik terimler açıklanmamıştır. Kapsamı geniştir, fakat bilgi ve iletişim güvenliği rehberindeki tüm kapsamları karşılamamaktadır. Belge kolay ulaşılabilir olmakla birlikte diğer bağımsız işletmeler tarafından isteğe bağlı uygulanabilir ve yine isteğe bağlı denetlenebilirdir.

Son olarak, diğer en geniş kapsamlı çerçeve ise Bilgi ve İletişim Güvenliği Rehberidir. Bu belge de denetim raporu gibi bazı kurum, kuruluşlar ve kritik bilgi taşıyan işletmeler için hazırlanmıştır. Esas belgesinin dışında bilgi ve iletişim güvenliği denetim raporuna da sahiptir. Bu sayede yine isteğe bağlı denetlenebilir ve sertifikalanabilirdir. Fakat tek başına bu rehber sertifika özelliğine sahip değildir. Dili genel olarak teknik değildir, fakat güçlendirme bölümlerinde teknik dil kullanılmaktadır. Bu da belgenin KOBİler açısından karmaşıklığını artırmıştır. Belge karmaşık olsa da, işletmeler tarafından kolay ulaşılabilecek durumdadır. Kolayca ulaşılıp, indirilebilir.

Güvenlik yapılarının karakteristik özellikleri tablo halinde verilmiş ve KOBİ'lere güvenlik mekanizmasına ulaşma yolunda yardımcı olması hedeflenmiştir. Ayrıca, detaylı kapsam analizleri ile, uygunluk ve kapsam seviyeleri de karşılaştırılmıştır. Detaylı kapsam karşılaştırılmasında, bu yapıların hangi kapsam maddesi üzerinde

hakim olduğu açıkca belirtilmiş ve derecelendirilmiştir. Belirtilen karşılaştırma adımları iki farklı tablo ortaya çıkartır. KOBİ'lerin güvenlik önlemleri yolunda bu iki tablo yardımcı olmayı hedeflemiştir.

Analizlerin tamamlanmasının ardından, KOBİ'lerin karşılaştığı saldırı türleri detaylı bir şekilde incelenmiş ve bu saldırıların kapsamlarına göre sınıflandırılması yapılmıştır. TÜİK raporuna göre, gelişmekte olan ülkelerden Türkiye'de 2022 yılında işletmelerin yaklaşık %28,5'i en az bir güvenlik ihlaline maruz kalmıştır. Dünya genelinde de bakılan iki farklı saldırı raporlarına bakıldığında bu oranın tutarlı olduğu görülmüştür. TÜİK raporunun ve bahsedilen diğer iki raporun incelenmesi sonucunda hizmet kesintisi, web sitesi engelleme, kimlik avı, veri ihlali, kişisel tanımlanabilir bilgi sızıntısı, kötü amaçlı yazılım ve yetkisiz erişim ana saldırı türlerindendir. Sınıflandırma ise bu atak türlerinin kaynaklarını ve önlemlerinin hangi güvenlik kapsamı ile ilişkili olduğunu belirtmekle bulunmuştur. İlişkilendirme sonucunda ağ ve sistem güvenliğinin %37,64, uygulama ve veri güvenliğinin %10,81, personel güvenliğinin %17,60, fiziksel mekanların güvenliğinin %17,10, kişisel veri güvenliğinin ise %16,83 oranında görüldüğü belirlenmiştir.

Analizlerle bulunan kapsam değerleri ve ataklara olan zaafiyeti açısından yaklaşım ile önceliklendirme çalışması yapılmıştır. Öncelik derecesi, atak sıklığı, kapsam kolaylığı ve kapsamın ağırlık derecesi ile bulunmuş ve karşılaştırılmıştır. Uygulamanın kolaylık değeri, karmaşıklık, finansal maliyet, zaman çerçevesi, kaynaklar ve uyum faktörleri ölçütlerine bağlı olarak belirlenmiştir. Ayrıca, her bir kapsam konusunun ağırlık katsayısı ise, risk ve potansiyel zararın değerlendirilmesine dayanmaktadır. Saldırı türlerinin güvenlik kapsamları ile ilişkisinden de yararlanarak, öncelik derecesi Saldırı sıklığı, ağırlık katsayısı ve kolaylığın çarpımı sonucunda bulunur. En iyi senaryoda bulunabilecek öncelik değeri 0,23 olmuştur. Yapılan hesaplamalar sonucunda ISO 27001 0,0469 ile en iyi senaryoya %20.002, NIST IR 7621 0,0987 ile en iyi senaryoya %42.032, Sayıştay BT denetim raporu 0,0581 ile en iyi senaryoya %24.748, bilgi ve iletişim güvenliği rehberi 0,0469 ile en iyi senaryoya %20 yaklaşmıştır. Buna dayanarak bu güvenlik yapıları NIST IR 7621, sayıştay BT denetim raporu, ISO 27001 ve Bilgi ve İletişim Güvenliği Rehberi olarak öncelik derecesine göre sıralanmıştır.

Bu bulguların yanı sıra karşılaştırma özelliklerine bağlı olarak farklı açılardan da sıralamalar ortaya çıkmıştır. Kapsam genişliğinin hiyerarşik sınıflandırması, KOBİ'lerin ihtiyaçlarına uygun olarak aşağıdaki gibi belirlenmiştir: ICSG, ISO 27001, TCA's IT Audit ve NIST IR7621. KOBİ'lerin seçebileceği yapıların karmaşıklık bağlamında hiyerarşik düzenlemesi ise NIST IR 7621, ISO 27001, ICSG ve TCA's IT Audit şeklindedir. Belirtilen sıralamalara ek olarak, sertifikasyon veya güvenlik yapılarının işletmelere sağlayabileceği güvenilirlik ve müşteri güveni avantajları açısından sıralama ISO 27001, ICSG, TCA's IT Audit ve NIST IR 7621 şeklinde bulunmuştur.

Ayrıca, tezde, kolay, maliyetsiz ve etkili güvenlik sağlama potansiyeline sahip birkaç öneri sunulmuştur. Bu öneriler, KOBİ'lerin bütçe kısıtlamaları içinde en uygun güvenlik çözümlerini bulmalarına yardımcı olacak şekilde ele alınmıştır. Ele alınan 5 maddelik öneri listesi, KOBİ'lerde en sık karşılaşılan saldırıların %72'sini kapsamayı vadetmektedir. Sonuç olarak, bu önerilerin de değerlendirildiği kapsamlı bir

derecelendirme sistemi, KOBİ'lerin ihtiyaçlarına en uygun bilgi güvenliği çözümlerini seçmelerine rehberlik etmek amacıyla sunulmuştur.

1. INTRODUCTION

Small and Medium-sized Enterprises (SMEs) constitute a cornerstone of the world's economies. SMEs provide a significant portion of employment and make substantial contributions to economic growth. According to the World Bank, SMEs constitute approximately 90% of enterprises and contribute to over 50% of global employment [1]. As a result of that, SME development is a high priority for many governments around the world. Also, this phenomenon extends beyond developed nations and applies to developing economies as well. For example, in Turkey, SMEs encompass 99.8% of all businesses, comprising 72% of the overall employment [2]. Furthermore, SMEs are at the heart of innovation and sustainability, playing a pivotal role. In order to protect themselves and ensure their sustainability, SMEs need to prioritize cybersecurity measures.

Millions of cyber attacks are initiated daily against global internet users. This also leads to various studies indicating that a person falls victim to an attack approximately every 39 seconds [3] [4]. SMEs are often targeted in cyber attacks due to their limited IT management, making them vulnerable [3] [5]. Needs for IT security required for IT management are budget, expertise, and awareness [5]. The organizations reporting at least one information and communication technology security incident in 2022 exhibited an increase as outlined: 27.8% for small-sized enterprises, 32.0% for medium-sized enterprises, and 34.1% for large-sized enterprises in Turkey [6]. Furthermore, according to the report compiled by MITRE, large enterprises experienced 496 incidents, whereas small businesses confronted a higher number, totaling 699 incidents [7].

Any attack or incident can have a significant impact on businesses. These impacts are outlined in the NIST document as follows: (i) damage to information or information system, (ii) regulatory fines and penalties / legal fees, (iii) decreased productivity, (iv) loss of information critical in running your business (therefore, loss of business

continuity), (v) an adverse reputation or loss of trust from customers, (vi) damage to your credit and inability to get loans from banks, (vii) or loss of business income [8]. Also, the impacts of the incidents have been stated in Gordon's Ph.D. thesis that cybersecurity on small to medium-sized businesses can result in adverse consequences, including diminished revenue, job losses, business closures, and reduced tax income [3]. These impacts extend beyond businesses, affecting local governments, employees, and consumers.

There are several ways to mitigate the risks and challenges faced by SMEs in the realm of cybersecurity. The thesis aims to evaluate and prioritize four different security measures, frameworks, for SMEs based on their risks and requirements. Notable frameworks include ISO 27001 and NIST IR 7621, globally recognized Information Security Management Systems (ISMS). In Turkey, the government has introduced the Turkish Court of Accounts (TCA)'s IT audit and Information and Communication Security Guide (ICSG) as security frameworks. Additionally, secondary objectives include proposing new recommendations in line with the identified needs and opportunities, which will be linked to the ranking, and providing SMEs with security measures recommendations. However, it is crucial to consider the limitations and constraints that SMEs face when implementing cybersecurity measures [9]. Furthermore, a thorough examination of the primary issue will involve a detailed analysis of risks and impacts.

1.1 Problem Definitions: SMEs Face Challenges In Various Aspects

SMEs are compelled to align their strategies with the unique needs of their organizations, ensuring the protection of assets, building credibility with users and governmental entities, and minimizing risks. The pervasive occurrence of security incidents within SMEs underscores the imperative for comprehensive security awareness initiatives. However, resource constraints may pose challenges for small businesses in developing or procuring sophisticated security systems.

1.1.1 Security

Most SMEs cannot afford effective security measures due to limited budgets, lack of information, or insufficient awareness. This situation is more prevalent in developing countries. For instance, 36.1% of startups in Turkey face difficulties in finding information and communication specialists. The reasons behind these challenges include (i) the lack of applications/inadequacy of candidates in the recruitment process, (ii) regulatory fines and penalties / legal fees, (iii) lack of qualifications (education/training) in the relevant field, (iv) their lack of relevant work experience, (v) or high wage expectations [6].

From a broader perspective, challenges encountered by SMEs in establishing security measures can be delineated as follows:

- SMEs could not find qualified employees or consultants.
- Qualified employees or consultants' costs could be out of reach.
- SMEs have lack knowledge of appropriate security measures.
- SMEs have a hard time comprehending security standards.
- SMEs cannot see the visible effects of the security measures in a short time. Long-term benefits are mostly overlooked and the budget to be spent cannot be rationalized.

1.1.2 Compatibility

While compliance with standard security requirements for SMEs may arise from the business's own initiative and benefit, mandatory situations can also compel compliance in terms of conformity. Therefore, SMEs may bear legal responsibilities. Governments or communities, with the aim of protecting the public or individuals, may seek certain guarantees from businesses under their jurisdiction. One of the most critical aspects is the protection of personal data. For instance, in Turkey, Personal Data Protection Law 6698 (KVKK), in the European Union, General Data Protection Regulation (GDPR),

and in the United States, Data Privacy Act are established. This can lead SMEs to require a security mechanism. Security frameworks adopted by businesses can also serve as guarantors in terms of privacy.

In brief, SMEs encounter challenges in accessing comprehensive and effective security guidance. Additionally, there is a lack of clarity regarding the specific requirements for cybersecurity. The absence of a readily available and easily understandable list of recommendations that SMEs can implement independently, without the need for external consultancy, exacerbates the situation.

1.2 Motivation

A multitude of scholarly investigations has been dedicated to evaluating the efficacy and comparative merits of security frameworks, with a distinct emphasis on their ramifications for SMEs. These inquiries, spanning diverse nations, underscore the critical significance of cyber hygiene and the nuanced calibration of security infrastructures designed to cater specifically to the distinctive requisites of SMEs. Gaitero et al., Kljucnikov et al., and Ncubukezi et al. have written articles for the benefit of their countries in security management systems for SMEs [10], [11], [12].

In addition, scholarly endeavors have undertaken comparative analyses of cybersecurity frameworks, extending their purview to regions such as the European Union and Indonesia. These studies contribute valuable insights into the variations and commonalities observed in cybersecurity structures across diverse geographical and regulatory landscapes [13], [14]. The primary objective is to conceptualize security certification for SMEs, shedding light on the subject through illustrative examples from Turkey while drawing insights from research conducted in Spain, Slovakia, South Africa and EU countries.

The Digital Transformation Office of the Republic of Turkey published The Information and Communication Security Measures and depending on these measures, the information and communication guidebook was released in 2019 after TCA's IT audit was published in 2013. The persistent endorsement of these two guides, coupled with the absence of adequate research in concerted endeavors, could potentially present

challenges for enterprises when deliberating on the selection of a security framework. The primary goal of the paper is to offer cost-effective self-assessment and practical security recommendations for SMEs worldwide. This is achieved through leveraging data from Turkey to evaluate the capabilities and comprehensiveness of SMEs' security management.

1.3 Solution Hypothesis

SMEs are particularly at risk due to limited resources for addressing cyber attacks, as well as a lack of cybersecurity knowledge among employees leading to low motivation to enhance cybersecurity practices. Larger companies' strengthened defense mechanisms against cyber attacks may make smaller organizations more likely targets. Therefore, less digitally mature SMEs could be extremely susceptible to cybersecurity threats. A comparative analysis will be conducted on four primary frameworks that businesses can utilize to address security vulnerabilities. Among the exemplars of ISMS, ISO 27001, renowned for its comprehensiveness, stands out, alongside NIST IR 7621, specifically tailored for SMEs. Additionally, the evaluation will encompass two prominent frameworks, namely ICSG and TCA's IT audit, which align with the legal obligations in Turkey. However, it is noteworthy that a considerable number of SMEs tend to experiment with a "fail-safe" approach, relying on various technical measures rather than implementing security policies. However, without much complexity introduced through certification programs or detailed investigation audit requirements, SMEs could mitigate several key cyber attacks by applying simple developing country-based self-assessment suggestions.

1.4 Contribution

The paper's contribution is bifurcated into two main facets. First, it encompasses the synthesis, comparison, and delineation of both commonalities and distinctions among the selected frameworks. This section serves to offer a comprehensive comparative analysis of the four frameworks under consideration. Second, the paper extends its contribution by presenting prioritized, cost-effective, and easily implementable security recommendations. The proposed recommendations strive to strike a balance

between financial and technical considerations while enhancing security. Additionally, the paper furnishes a systematic list of countermeasures prioritized according to their efficacy against prevalent security incidents.

1.5 Organization of the Thesis

This thesis contains 7 chapters. In Section 1, the main problem, motivation, and goals of this study are explained. In Section 2, current information about framework comparison methods and analysis, and security aspects of SMEs are given. In Section 3, the aforementioned frameworks are described and analyzed. Moreover, the comparison is based on the analyses accomplished. In Section 4, common attack types are analyzed and matched with the specified scope items. In Section 5, the mentioned frameworks are rated based on attack frequency, the intensity of specified scope items, and the ease-of-implementation values of these items. Using this scoring system, the frameworks are ranked. Additionally, independent strategic measures that are both easily implementable and capable of providing sufficient security are provided. In Section 6, the functionality of the provided security measures, as well as the positive or negative situations created by the security framework are interpreted. In Section 7, the benefits of this study are discussed.

2. LITERATURE REVIEW

In the literature, there are numerous and comprehensive studies on both comparisons of cybersecurity frameworks and security awareness and measures for SMEs. In this thesis, the literature review will be divided into two main categories. Methods, results, and reports of the studies will be discussed.

2.1 Comparison Reviews

While comparative articles are becoming increasingly popular, the most well-known ISMS method, ISO 27001, is featured in most of these articles. These articles include some distinguishing points. They are divided into four categories: the documents compared, the relevant country where the comparison is applied, the target audience, and the extracted results.

In comparative articles, detailed content comparisons and scope mappings could be observed. For instance, in the paper of Kurii and Opirskyy, ISO 27001 and NIST SP 800-53 are thoroughly analyzed, and a scope comparison is conducted [15]. On the other hand, Roy's paper compares NIST CSF and ISO 27001 [16]. While Roy outlines the advantages and disadvantages of both structures, the conclusion of both studies indicates that they are purely analytical, and neither study proposes a specific framework [16]. Therefore, due to these reasons, the target country or audience has not been specified. Additionally, Alshar's comparative study is for framework selection in that NIST CSF and ISO 27001 have been thoroughly examined, and the weaknesses, strengths, and organizational needs of the specified frameworks have been delineated [17]. Similarly, a specific size or region of the enterprises has not been targeted.

Sulistyowati et al. compared NIST CSF, COBIT, ISO/IEC 27002, and PCI DSS standards to design a cybersecurity maturity assessment methodology [18]. The paper focuses on focus areas, functions/ objectives, and categories/ subcategories of the frameworks. Furthermore, it places particular emphasis on the analysis and mapping

of content within its scope. Consequent to the comparative analysis, the authors have proffered 21 categories suitable for evaluating the cybersecurity maturity of ABC organizations [18]. Nonetheless, contingent upon the extent of the scrutinized framework, its applicability may extend to a diverse array of organizations, albeit with potential limitations regarding its relevance to SMEs.

On the other hand, Dewanto's study compares information security assessment models for the Indonesian government [14]. In the study, detailed analyses of ISO 27001 and the government-accepted KAMI index are conducted. As a result, the paper illustrates their reliability and accuracy in assessing the maturity and readiness of information security in government agencies in Indonesia. Therefore, the authors proposed two evaluation models designed for the Indonesian government.

Another study [19] under consideration is a paper that conducts analyses on security standards, professional certifications, and technological tools for information security practice, identifying their roles. The paper does not explicitly mention specific security standards. However, the frameworks, NIST SP 800 series, PCI DSS, ISO/IEC 27000 series, SSAE 16, COBIT, and ITIL frameworks have been assessed by analysts and managers in terms of requirements and preferences, revealing significant structures. The conclusions indicate that organizations prioritize knowledge verified through professional certifications and practical familiarity with IT products and solutions more highly than knowledge specific to a particular security standard in the context of information security management from the perspective of companies in job postings.

Some comparative articles have also focused on SMEs. Teufel's study and the European Union Agency for Cybersecurity (ENISA) report, in particular, concentrate on detailed comparisons of structures from the perspective of SMEs. The Cybersecurity For SMEs Challenges and Recommendations is ENISA's report for SMEs. The report [13] conducts a detailed comparison of the security frameworks utilized in the European Union, addressing the challenges faced by SMEs and underscoring the apparent lack of guidance in the midst of these difficulties. It mostly focuses on the challenges and recommendations for SMEs. The document furnishes concrete outcomes and suggestions aimed at fortifying the cybersecurity

stance of SMEs, giving attention to technical, organizational, and policy facets. While this report is extensive and pertinent to SMEs, the proposed recommendations may pose challenges for implementation, particularly in developing nations, due to potential costs and complexities. Also, Teufel's study [20], akin to the report [13], systematically constructs a new security canvas in five steps by comparing ISO 27001, BSI IT-Grundschutz Catalogues, and NIST framework. This canvas, designed for SMEs, rates concepts as mandatory, strongly recommended, and recommended. In this respect, this thesis work shares similarities, albeit with distinctions in the structures compared and the target audience.

2.2 Cyber Security Approaches for SMEs

The study [21] aims to assess the efficiency of cybersecurity procedures in small businesses in Saudi Arabia when facing cyber attacks, with a focus on financial impact, loss of confidential information, and recovery time. Besides, the paper found that financial damage caused by cyber-attacks could be limited by having an inspection team and recovery plan. Furthermore, the research has revealed that awareness is a crucial factor in preventing the loss of personal and significant information.

Also, in the Nordic-Baltic Region, the paper [9] analyzes cyber security challenges for SMEs. Moreover, Falch et al. proposed the technical and organizational tasks that SMEs can perform to ensure cybersecurity [9]. In formulating these tasks, consideration was given to NIST's methodologies in safeguarding enterprises, along with the analysis of security measures in the European and Baltic Sea regions.

Strategic Cybersecurity Risk Management practices for information in small and medium enterprises is an extensive research study on risk management. The study [22] delves into various aspects, including structures employed in information security, solutions cited from other research articles, and proposed recommendations from the literature. Additionally, utilizing the Delphi data collection method, surveys were conducted, and based on the results, a risk management analysis was formulated specifically for SMEs. The analysis results indicate the necessity of certain methods, while also highlighting areas where new solutions could be introduced.

Another study [23] proposed a valuable method called SMECRA (SME Cyber Risk Assessment). This methodology is for evaluating cyber risks and supporting cyber-security investment decisions which enables SMEs to make judicious cybersecurity investment decisions based on informed assessments.

The article [12] is tailored for SMEs, cyber hygiene has emerged from the challenges faced by SMEs and the detailed depiction of deficiencies in cybersecurity rules and structures. Ncubukezi et al. compile recommendations that SMEs should undertake for cyber hygiene, with a focus on employee education and training [12]. Also, Talu's study [24] emphasizes employee training programs to raise awareness and backup systems in order to understand cybersecurity management in micro and small enterprises (MESEs) in Europe.

3. OVERVIEW AND COMPARISON BETWEEN AFOREMENTIONED FRAMEWORKS

In this chapter, details of the aforementioned frameworks are described. The frameworks contain some distinguishing key points to fulfill cybersecurity needs. According to the comparison studies, the key features are description, structure, mechanism, scope, business flow, certifiable, mandatory documents, complexity, target organization, and availability [16], [17] and [15].

Description: A description provides information about the purposes for which a structure is established and the promises it offers to the target audience. User awareness of this information fosters an understanding of the structure in question.

Structure: The differentiation of the frameworks can be facilitated by examining the document structure, which should strive for simplicity, directness, and a user-friendly interface in order to enhance comprehension of security measures specifically designed for SMEs.

Mechanism: Mechanism is another perspective for diversing frameworks. It provides information about how the system's mechanism operates. This, in turn, leads us to an understanding of how manners are assessed.

Scope: A comprehensive security framework integrates both physical and logical security components, thereby supporting sustainability goals and preventing redundancies and significant security deficiencies [25]. Comprehensive security management systems that encompass all security policies may incur significant costs and demand a substantial investment of time. Conversely, security management systems with a limited scope may not adequately safeguard organizations and could potentially give rise to security vulnerabilities. In order to strike a balance between these two considerations, it is imperative for security systems to possess a meticulously planned and carefully defined scope.

Business Flow The business flow develops in accordance with the semantic and strategic structure of each framework. This criterion should align with the needs of customers, other organizations, and governments utilizing the frameworks to enhance resilience against cybersecurity attacks.

Certifiable: Certification based on a given framework is important as proof of the reliability of SMEs. Although this may come at a high cost, there is a possibility that it may assist the organization in gaining the trust of its stakeholders and consumers [17]. Certifiable features in cyber security frameworks are important because they provide alternative education, help with job requirements, and ensure employees gain knowledge on recent trends and technologies [26]. Moreover, having a certificate attracts new businesses, and government-based agreements become more accessible.

Mandatory Documents: The mandatory documents constitute a set of documentation that includes forms, processes, and tests that must be fulfilled for certification. While making them mandatory aims to assist in the certification process, it may, however, give rise to cost-related issues.

Complexity: The complexity point denotes the technical level and level of difficulty of the structure. It is recommended not to propose overly technical information and complex structures for SMEs in terms of cost and implementation time.

Target Organization: The suitability of the frameworks for the intended audience is determined by their applicability. The selection of a framework may also depend on the type of business or industry, including factors such as size, sector, and location. Businesses are inclined to select a framework based on their specific sector or size.

Availability: The point of Availability provides information on how access to the document or certificate can be achieved. Being easily accessible is again a preferable aspect for SMEs.

3.1 ISO 27001

ISO 27001 is a globally accepted standard for information security, cybersecurity and privacy protection. ISO 27001 seeks to establish a benchmark for the management of information security by addressing aspects such as motivations, challenges in implementation, potential outcomes, and contextual factors [27]. Therefore, this certification aims to tackle worldwide cybersecurity challenges and enhance digital trust. The ISO 27001 standard stands as one of the most extensively adopted frameworks globally, serving as the foundational standard within the ISO/IEC 27000 family of standards [28] [29]. The third edition of this standard, which adapts to innovations, was released in October 2022.

The ISO 27001 standard confronts global challenges in cybersecurity and enhances digital trust for enterprises on a worldwide scale [28]. It is widely acknowledged and employed as the primary cybersecurity and risk management framework within numerous organizations spanning nearly all countries globally. ISO 27001 accommodates customized applications to meet the distinct and specific requirements of businesses due to its flexibility. This aspect enables the standard to cater to enterprises of various sizes and industries [30]. In other words, the standard could be implemented in any kind of organization, profit or nonprofit, private or state-owned, small or large [15].

One of the most significant features of this standard is its capability for certification. The certification attribute aims to eliminate issues related to reliability. The adoption of ISO ensures the reliability, constant availability, and security of data [17]. The ISO 27001 certification process is conducted by independent certification bodies. The independent auditor's role is divided into two main aspects. The first involves scrutinizing whether the procedures, policies, or methods outlined in the ISO 27001 clauses are being implemented. The second step entails verifying compliance with the controls specified in Annex A (ISO 27002) [17] [31]. Upon the completion of these two steps, organizations become eligible for certification. However, these certifications are required to be renewed every three years.

ISO 27001 standard includes specifications for installation, performance, operation, controlling and monitoring, review, maintenance, and improvement of the system [29] [17]. Also, the standard contains practices, methods, and processes similar to other ISMS. ISO 27001 comprises methodological requirements and security control requirements, structured within the Plan-Do-Check-Act (PDCA) model for the former and the ‘subject access object‘ model for the latter [32]. This standard comprises 11 sections and an additional Annex A with 93 items. These sections are also known as clauses. While Clauses 0–4 may not appear obligatory for ISMS, Clauses 4 through 10 are recognized as mandatory for ISMS, constituting 7 essential items for certifications. Clauses denote the compulsory elements in management systems, whereas the controls in Annex A are designed to implement cybersecurity controls [28]. The mandatory clauses of this standard as a framework could be listed as; (i) Context of organization, (ii) Leadership, (iii) Planning, (iv) Support, (v) Operation, (vi) Performance evaluation, (vii) Improvement.

On the other hand, the scope of security measures is determined by the content of Annex A. In the ISO 27001:2013, 2nd edition, the security scope comprises 114 items grouped as follows:

- Risk Assessment
- Security Policy
- Organization of Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Management
- Information Systems Acquisition Developments and Maintenance
- Information Security Incident Management

- Business Continuity Management
- Cryptography
- Supplier Relationships
- Compliance

In the 3rd edition of the standard, there are 93 items. However, in this context, there has been no scope loss; instead, certain items have been consolidated. Additionally, 11 new security measures have been introduced. These are (i) Threat intelligence; (ii) Information security for the use of cloud services; (iii) ICT readiness for business continuity; (iv) Physical security monitoring; (v) Configuration management; (vi) Information deletion; (vii) Data masking; (viii) Data leakage prevention; (ix) Monitoring activities; (x) Web filtering; (xi) Secure coding [28]. Finally, the grouping method has been reduced from 14 to 4, which signifies the representation of our scope. The presented scope could be listed as:

- organizational dimension
- people dimension
- physical dimension
- technological dimension

Due to its flexible structure, ISO 27001 is noted in various researches as being applicable to businesses of every size and sector. Owing to this structure, certain records and documents are categorized as mandatory, while others are non-mandatory. Businesses aspiring to attain this certification are unable to do so without fulfilling the mandatory document requirements. Some of these documents include the ISMS Scope document, Information Security Policy, Risk Assessment Report, Statement of Applicability, and Internal Audit Report. In addition to these, there are 10 more mandatory documents and 7 mandatory records [33].

ISO does not explicitly detail its scopes. The frequent use of the term ‘shall‘ in cybersecurity measures, while making the language of the mentioned structure less

technical, necessitates budget allocation for IT [17] [15]. This situation, while reducing the complexity of the structure, also increases cost-related challenges.

Additionally, the ISO 27001 framework is commercially distributed through the official website [15]. Moreover, after achieving ISO 27001, the implementation process may necessitate the involvement of a consultant or platform, both of which could be costly. In addition, the certification process itself incurs expenses that can amount to tens of thousands of dollars. The renewal process is also an additional cost. Consequently, obtaining this certification could be highly expensive and challenging. This appears as a negative feature for ISO 27001 in terms of cost.

3.2 NIST IR 7621

NIST IR 7621 is a guide based on the Framework for Improving Critical Infrastructure Cybersecurity [CSF14] template within the NIST framework, providing simple security measures for SMEs. This guide articulates security measures for information, system, and network security in a non-technical language specifically tailored for SMEs. The targeted organizations have been stated in the framework as Small Enterprises or Small Organizations and include for-profit, non-profit, and similar organizations [16].

Like all other NIST frameworks, NISTIR 7621 is voluntary. Therefore, lacking a certification feature, it relies on self-assessment and self-compliance. Due to its self-certification nature, no specific IT expertise is required. It is not controlled or managed by an outside authority.

The business cycle of the framework identifies what information the business stores and uses, determines the value of the information, develops an inventory, and understands the threats and vulnerabilities [16]. The workflow consisting of identification, protection, detection, response, and recovery represents the structure's five core categories within NIST IR 7621. Additionally, this structure encompasses 20 subcategories. The content of this structure, which has a limited scope, covers

- physical security,
- personnel security,

- contingency planning and disaster recovery,
- operational security,
- and privacy.

General controls include restricting employees' access to data and information, providing cybersecurity training for employees, establishing policies and procedures for information security, encrypting data, implementing web and email filters, and patching or updating operating systems and applications [34]. In addition to these controls, it includes recommendations such as performing backups, downloading cybersecurity software, purchasing cybersecurity insurance, and finding reputable cybersecurity contractors [34].

The best practices are listed as Antivirus, Internet Security, Firewall, Patching, Backups, Physical Security, Wireless Security, Employee Awareness, Individual User Accounts, and Limiting Access. It is believed that these measures also provide solutions to common issues such as Email Security, Web Security, Pop-up Windows, Online Business, Hiring Practices, Downloading Software, Web Surfing, Getting Help, Equipment and Media Disposal, and Social Engineering [35].

Due to the absence of a certification feature, there are no mandatory documents. The original document includes a glossary, definitions, applications, and worksheets for risk analyses as sample descriptions in the annexes. The descriptions of the structure and annexes in the original document are as follows:

- Section 2 describes how an information security program can be implemented
- Section 3 discusses the key actions small businesses can take to develop or improve
- Section 4 identifies several key practices directed towards users which you can implement immediately and which will protect your system and information
- Appendix A provides a glossary of key terms and acronyms used in this publication
- Appendix B contains sources referenced throughout this publication

- Appendix C contains a description of the NIST Framework for Improving Critical Infrastructure Cybersecurity [CSF14]
- Appendix D provides worksheets useful in conducting a risk analysis
- Appendix E contains example information security policy and procedure statements on their information security and cybersecurity

NIST IR 7621 is specifically designed for small businesses, characterized by a narrowly scoped structure encompassing a non-technical language and simple security rules, thereby exhibiting a straightforward and uncomplicated framework. Additionally, this structure is easily accessible. It can be freely downloaded and implemented from the official website of NIST.

3.3 TCA's IT Audit

The Information Systems (IT) Audit Guide was developed by the Turkish Court of Accounts in 2013 with the aim of providing guidance to auditors on how to plan, execute, and report on information systems audits. The audit has emerged with the aim of identifying vulnerabilities, providing recommendations, and disseminating information to prevent financial issues that may arise from cybersecurity problems.

This framework is designed to be applied to entities that need to undergo financial audits in accordance with the requirements of the TCA. However, it can be implemented for any type of information system seeking an audit. Structured with a focus on enabling auditors specializing in the field to prepare reports, the guide delineates, step by step, the tasks a specialized auditor needs to perform. In this regard, the guide emphasizes the aspects of cybersecurity that businesses need to consider.

This structure does not possess a certification feature. The audited business can ascertain the status of its audit quality through the report of findings generated by the auditor. Additionally, the business will have a detailed report addressing areas that require correction.

The framework is supported by practical examples from various countries and similar institutions. While ISO standards stand as the primary source, INTOSAI guidelines

and standards, along with ISACA guides, play a significant role in the preparation of the relevant structure [36] [37] [38]. All the resources utilized in the preparation of the guide are as follows: COBIT[1], ISO/IEC 27000 [2], ISO/IEC 38500 [3], ITIL [4], TOGAF [5], PMBOK [6], ISO/IEC 15408 [7], and NIST SP800 [8] [38].

The process will unfold as follows: (i) initially identifying the risks associated with the examined information system, (ii) determining control mechanisms to minimize these risks, (iii) assessing whether these control mechanisms are created, taking into account the organization's structure, and evaluating their effectiveness, (iv) post-examination, evaluating weaknesses in internal controls, and (v) reporting the findings according to a specified procedure [36].

The structure of TCA's IT audit encompasses audit planning, system controls and evaluation, and audit result reporting and monitoring. Additionally, these three categories encompass topics such as;

- management controls
- physical and environmental controls
- network management and security controls
- logical access controls
- operational controls
- system development and change management controls
- emergency and business continuity planning controls

TCA's guide, like other audits, harbors certain concerns, which can be addressed through procedures and practices. Among the provisions of this framework are general

[1] https://www.isaca.org/resources/cobit
[2] https://www.iso.org/standard/73906.html
[3] https://www.iso.org/standard/62816.html
[4] https://www.axelos.com/certifications/itil-service-management
[5] https://publications.opengroup.org/standards/togaf/specifications/c220
[6] https://www.pmi.org/pmbok-guide-standards/foundational/pmbok
[7] https://www.iso.org/standard/72917.html
[8] https://csrc.nist.gov/pubs/sp/800/225/final

access, policies on virtual private networks and network device security, guidelines for internet usage, and user security measures [39]. Additionally, it encompasses procedures on various topics, including protection against malware, monitoring for compliance, antivirus policies, vulnerability detection, authentication, authorization, maintenance plans, personal records security, and crisis management [39].

The TCA audit requires the completion of several mandatory annex forms. These forms include the information systems information form, account fields affected by IT systems determination form, system risk assessment form, risk assessment matrix, and evaluation form, findings/ risks assessment matrix, and the information systems audit quality control form [36]. The purpose of these forms is to assess the audit with oversight from an authoritative body.

Although lacking a certification feature, this structure, given its auditing purpose, requires certain mandatory documents. As a result of the documents filled out by expert auditors designated by TCA, there will be a scoring system in the report section. The mandatory documents specified in this structure are as follows: information systems information form, account fields affected by IT systems determination form, system risk assessment form, risk assessment matrix, and evaluation form, findings/ risks assessment matrix, and the information systems audit quality control form [36].

The guide is prepared under the assumption that it will be used by auditors specialized in information systems auditing, who have a certain level of knowledge about concepts related to information systems auditing. Therefore, conceptual explanations are kept to a minimum. In terms of scope and language, it is advisable for businesses to allocate a budget for IT. This guide can be freely downloaded from the official website of the Court of Accounts.

3.4 Information and Communication Security Guide

The Guide for Information and Communication Security has been developed by the Presidency of the Republic of Turkey, Digital Transformation Office, in the context of the Information and Communication Security Measures Directive numbered 2019/1, encompassing information and communication security measures. This guide,

established through the efforts of the same ßregulatory body, aims to enhance the level of information security nationwide at the legislative regulation level. The purpose of this guide is to reduce and mitigate security risks, particularly safeguarding the security of critical data that, when compromised in terms of confidentiality, integrity, or accessibility, could pose a threat to national security or disrupt public order. The framework is tailored to the country's regulatory framework and unique needs. Adherence to this guide is obligatory for public institutions and enterprises providing critical infrastructure services [40].

The Information and Communication Security Guide does not possess a certification feature. However, in order to achieve and sustain the targeted outcomes of the mentioned guide, the Turkish Presidency's Digital Transformation Office published the Information and Communication Security Audit Guide in October 2021. The audit guide is written for independent auditors following the guidelines of the information and communication security guide. To become an auditor for this guide, the Turkish Presidency's Digital Transformation Office provides TSE-approved training and certifications. Furthermore, as part of the auditor's required competencies, the inclusion of the ISO/IEC 27001 Lead Auditor Certificate is noted [41]. This enables public institutions, organizations, and businesses providing critical infrastructure services to obtain certification from the Information and Communication Security Guide.

The 12 objectives of the Information and Communication Security Guide, as outlined within the guide, are as follows: Encouragement of local and national products, prevention of redundant work and investments, different security levels, applicability, traceability, technological independence, audibility, modularity, originality, sustainability, multipurpose functionality, and compatibility [40].

The guide, which is compliant with numerous laws and regulations, draws on various sources, primarily relying on CIS, NIST Framework for Improving Critical Infrastructure Cybersecurity, NIST IR 8228, OWASP, PCI DSS, and ISO 27001 frameworks as its foundational pillars. The implementation process of this guideline

involves planning, implementing, controlling, and preventing, as well as change management.

This framework is compartmentalized into five distinct sections: introduction, the application process of the information and communication security guide, security measures tailored for asset groups, security measures focusing on application and technology domains, and stringent measures. The guide encompasses procedural steps like inventory determination within the implementation phase, with the remaining sections forming the overall scope. The scope is meticulously analyzed under three primary headings, as delineated in the guide's sections. (i) Network and system security, (ii) application and data security, (iii) removable devices and media security, (iv) Internet of Things (IoT) security, (v) personnel security (vi) physical environment security are under the Security measures for asset groups. While (i) security of personal data, (ii) instant messaging security, (iii) cloud security, (iv) security of crypto applications, (v) critical infrastructure security, and (vi) new developments and supply are under the Security measures for application and technology areas, (i) operating system hardening, (ii) database hardening, and (iii) server hardening are under the hardening measures.

The guide, lacking inherent certification attributes, primarily contains supplementary appendices and documents within its content. Conversely, the Information and Communication Security Audit Guide incorporates ten mandatory forms and documents. On the other hand, the guide includes certain definitions and is structured in a comprehensible, non-technical language for ease of understanding. However, the intensity of the scope has increased complexity. Additionally, accessibility remains straightforward, as the guide, audit report, and relevant decree could be easily downloaded and implemented from the official website of the Turkish Presidency Digital Transformation Office.

3.5 Comparison

Eleven points considered crucial when selecting the security structure for enterprises have been outlined. When examining the descriptions of the mentioned frameworks, it is evident that all structures aim to address issues related to information security,

cybersecurity, and privacy. However, they differentiate themselves in terms of global recognition and acceptance, as ISO 27001 is globally recognized, NIST IR 7621 is tailored for small businesses, TCA's IT audit focuses on financial concerns, and the Information and Communication Security Guide aims to elevate the security of Turkish public and institutions to a global level. The comparison based on the given 11 parameters and detailed structure analyses is presented in Table 3.1.

However, the target audience of the aforementioned frameworks varies. ISO 27001 offers a flexible structure suitable for businesses of all sectors and sizes, catering to a broad audience. On the other hand, NIST IR 7621 is designed to address the specific needs of small businesses, both for-profit and non-profit, as well as similar organizational structures, focusing on a more specialized audience. TCA's IT audit and ICSG, on the other hand, are crafted for public institutions, organizations, and businesses handling critical information within Turkey. However, both frameworks emphasize that their objectives are applicable to any business willing to implement them.

Certification and its mechanism are also two significant points to consider. While the certification feature enhances reliability, it should be noted that it incurs costs for small businesses. Among the aforementioned frameworks, only ISO 27001 has a certification feature. TCA's IT audit and ICSG can be considered semi-certifiable and have an audit-based mechanism. The report result in TCA's IT audit, due to financial reasons, can be perceived as a partial certificate. ICSG, by its structure, is not certified but can be optionally certified with the ICS audit guide. All the mentioned frameworks are audited by independent auditors. NIST IR 7621, on the other hand, is a completely optional structure that can be applied, thus possessing a self-certificate feature.

The operational cycles of these frameworks can be explained in three different ways. The Plan, Do, Check, Act (PDCA) cycle is utilized by ISO 27001 and ICSG, while the Plan, Control, Evaluate, and Report (PCER) cycle is employed by TCA's IT audit. NIST IR 7621 utilizes the Identify, Protect, Detect, Respond, Recover (IPDRR) cycle. The selection of these frameworks depends on the preferences and strategies of the businesses.

The structure of the frameworks could be distinguished by the sections they are divided into. Additionally, the readability and complexity of the security frameworks can be assessed in conjunction with the structure of these aforementioned frameworks. For instance, ISO 27001 consists of 11 sections, TCA's IT audit has 3 sections, and ICSG has 5 sections. All of these structures are presented in a tabulated form. ISO 27001 and ICSG avoid using technical language and provide explanations. However, in the hardening measures, the language is technical. TCA's IT audit is presumed to be familiar to auditors since it is prepared for them. On the other hand, NIST IR 7621 comprises 5 main categories and 20 subcategories, presented in the form of a recommendation list instead of a tabulated form. Despite the attempts of the other frameworks to avoid technical details, NIST IR 7621 is the most readable and straightforward structure.

The scope sections of the frameworks also differ in a manner similar to their structures. While many of them suggest similar precautions, the way these precautions are expressed varies across the documents. Therefore, in the scope comparison, the primary criterion will be the number of items included, and a detailed comparison table will be provided in Table 3.3. In the mentioned frameworks, ISO 27001 has four scope items, NISTIR has six scope items, TCA's IT audit has seven scope items, and ICSG has 15 scope items, respectively. In addition, the mandatory documents required to obtain certification are included in the content of the frameworks. ISO 27001 requires six forms and six records, while TCA's IT audit includes 12 mandatory documents. Since the other frameworks lack certification features, there are no mandatory documents associated with them.

Finally, accessibility and easy access play a pivotal role in selecting a security framework for SMEs. In this regard, ISO 27001 is only accessible through its official website for a trade-based fee, while the other three frameworks can be easily downloaded from their official sites.

Table 3.1 : The document outlines of ISO 27001, NIST IR 7621, TCA's Audit, and Information and Communication Security Guide

	ISO 27001	NIST IR 7621	TCA's IT Audit	ICSG
Description	a globally accepted standard for information security, cybersecurity and privacy protection	security measures for information, system, and network security tailored for SMEs	accepted audit for cybersecurity problems to prevent financial issues	guide for enhancing the level of information security nationwide at the legislative regulation level
Target Organization	all types and sizes	Small Business	public institutions, organizations	public institutions, organizations, and businesses
Certification	Yes	No	Partial	Partial
Mechanism	independent audit based	voluntary, self-certification	audit based	audit based
Business Flow	PDCA	IPDRR	PCER	PDCA
Structure	11 Sections	5 Core Categories	3 Section	5 Section
Scope	4 Matters	5 Matters	7 Matters	15 Matters
Mandatory Documents	6 documents and 6 records	None	12 Required form	None
Technological Neutrality	yes	yes	yes	yes
Complexity	less technical, but require IT	non-technical language	technical, but require auditor	technical in hardening scopes
Availability	Distributed on a commercial basis through the official website	Can be freely downloaded from official source	Can be freely downloaded from official source	Can be freely downloaded from official source

3.5.1 Detailed scope comparison

Depending on the scope perspective, many similarities exist in between the aforementioned four documents. (i) Physical security is one of them. The protection of the property or physical assets like using locks or cameras is a crucial point of security. The given four structures include physical security. (ii) Personal security is defined in ISO 27001 as Human Resources security. Also, personal security is placed in management controls in the TCA audit. Management controls include strategic planning, security policies, organization, asset management, personnel and training policies, and regulatory compliance. However, the details of personal security in each security structure are different. (iii) Operational security is placed in ISO 27001 as a Communications and Operations Management and in TCA audit as an Operational Control. In addition, all of the security frameworks consist of risk management and disaster recovery under different names. As a result of these facts, the grading system is used for scope comparison.

As a detailed framework for all organizations, irrespective of their size, type, or nature; ISO 27001 and Information and Communication Security Guideline have a more detailed scope than the others. For this reason, the paper uses the Information and Communication Security Guideline as a baseline for 3.3. Certificates' scopes are scored between 1 and 5 being the most effective in the grading system akin to the system of TCA's IT audit. The grading criteria are placed in Table 3.2.

Table 3.2 : The Grading Criteria

Grade	Meaning
1	not available
2	insufficient
3	mentioned
4	sufficiently referenced
5	thoroughly detailed

The first scope of ICSG, network and system security, covers subtopics such as (i) hardware asset inventory management, (ii) software asset inventory management, (iii) threat and vulnerability management, (iv) email server and client security,

(v) protection against malicious software, (vi) network security, (vii) data leakage prevention, (viii) logging and monitoring of traces and audits, (ix) virtualization security, (x) cybersecurity incident management, penetration testing and security audits, (xi) authentication and access management, (xii) disaster recovery and business continuity management, and (xiii) remote work.

In ISO 27001, full coverage is achieved through the measures specified in the sub-controls of the scopes: (i) asset management, (ii) communications and operations security, (iii) access controls, (iv) cryptography, and (v) information security incident management. Also, The scope of Network Management and Security Controls in TCA's IT audit aligns with various subtopics, although it does not encompass measures such as Virtualization and Remote Work. For this reason, TCA's IT audit sufficiently references the network and system security scope. However, despite being insufficient in this scope, NISTIR provides certain preventive measures like installing and activating software and hardware firewalls on all business networks, securing wireless access points and networks, and setting up web and email filters, addressing aspects such as Network Security and Email Server and Client Security. The scope of NIST IR 7621 is insufficient.

The scope of Application and Data Security encompasses subcategories such as Authentication, Session Management, Authorization, Security of Files and Resources, Secure Installation and Configuration, Secure Software Development, Database and Record Management, Error Handling and Record Management, Communication Security, Prevention of Malicious Operations, and Security of External System Integrations. ISO 27001 incorporates these subcategories within the scope of the following main categories: system acquisition, development and maintenance, access control, operations security, and supplier relationships. TCA's IT audit covers this topic under the management controls section, specifically addressing security policies. NIST IR 7621 covers application and data security extensively as it addresses the main subtopics related to authentication, authorization, and database and record-keeping methods.

The subtopics of Portable Device and Environmental Security scope include Smartphones and Tablet Security, Portable Computer Security, and Portable Media Security (CD/ DVD, Portable Memory Environments). These subtopics are also addressed within the ISO 27001 framework under the headings of Organization of Information Security, Asset Management, and Operations Security. However, the scope which is portable devices and environmental security, is not available in neither NIST IR 7621 nor TCA's IT audit.

The scope of Internet of Things (IoT) Device Security includes Network Services and Communication, Internal Data Storage, Authentication and Authorization, API and Connection Security, and Other Security Measures. In ISO 27001, these controls are addressed within the access control and communication security scopes and have been further developed 3rd version of ISO 27001 in 2022. However, this scope is not addressed by NIST IR 7621 and TCA's IT audit.

Security measures under the Personnel Security main heading are divided into General Security Measures, Training and Awareness Activities, and Supplier Relationship Security. ISO 27001's human resource security and supplier relationships scopes cover the mentioned subheadings. Additionally, TCA's IT audit's personnel and training policies under the main heading may encompass General Security Measures, Training, and Awareness Activities. NIST IR 7621 also mentions this security scope with the suggestion "Train your employees".

The scope of Physical Environment Security is divided into General Security Measures, Security Measures for the System Room/ Data Center, and Methods for Protection Against Electromagnetic Information Leakage (TEMPEST). This scope corresponds to the physical and environmental security scope in ISO 27001. Additionally, TCA's IT audit's physical and environmental security scope corresponds to General Security Measures and Security Measures for the System Room/ Data Center. This largely aligns with each other. NIST IR 7621 also contains recommendations equivalent to general security measures. In summary, this scope is present in NIST IR 7621 but it is not sufficient.

The lists of measures taken within the framework of personal data security are present in all structures. Key precautionary headings for the security of personal data include record management, access log management, authorization, encryption, backup, deletion, destruction, and anonymization. Considering that the security of personal data is protected by legal laws and regulations and involves privacy, additional measures such as Compliance with Legal Obligations such as Information Management, Explicit Consent Management, and Operation of the Personal Data Management Process may be present. The scopes of operations security, system acquisition, access control, development and maintenance, and compliance with legal and contractual requirements, and Information security reviews subtitles, encompass detailed personal data security within ISO 27001. This comprehensive section of the ISO 27001's structure addresses legal requirements as well. However, TCA's IT audit and NIST IR 7621 do not address legal requirements. The framework, TCA's IT audit, which has scopes that are logical access controls, management controls, and operational controls sufficiently referenced personal data security. Also, NIST IR 7621's scope mentions the personally identifiable information with a couple of suggestions. The recommendations include:

- Identify and control individuals with access to your business information,
- Mandate individual user accounts for each employee,
- Establish policies and procedures for information security,
- Restrict employee access to data and information,
- Implement encryption for sensitive business information,
- Formulate a plan for managing disasters and information security incidents,
- Conduct incremental backups of crucial business data/information, and
- Refrain from disclosing personal or business information.

Instant messaging security is addressed within the comprehensive scope of ISO 27001, encompassing various control measures under its access control and cryptography

scope items. However, TCA's IT audit and NIST IR 7621 do not explicitly include this aspect in their scope.

Similarly, Cloud security is also encompassed by ISO 27001 under the roof of access control and supplier relationships scope items. Also, ISO 27001:2022 has further enhanced these controls. Cloud security is not available in TCA's IT audit and NIST IR 7621.

The main control title, Cryptographic Algorithms and Usage, Encryption and Key Management, and Cryptographic Applications, under the heading of Cryptographic Applications Security, is equivalent to the cryptography scope in ISO 27001. However, this specific scope is not present in TCA's IT audit and NIST IR 7621.

In ICSG, all security measures specific to the energy and electronic communication sector to be implemented under the Critical Infrastructure Security scope are included. This encompasses Network and System Security, Application and Data Security, Security of Portable Devices and Environments, Security of Internet of Things (IoT) Devices, Personnel Security, and Physical Environment Security. In other frameworks, these measures are distributed across various scopes.

On the other hand, supply chain security in ICSG overlaps supplier relationship controls in ISO 27001. However, the inclusion of specific rules such as Turkish language support and comprehensibility tailored for Turkey's public institutions distinguishes ICSG in this scope. There is no control over supply chain security in both TCA's IT audit and NIST IR 7621.

Hardening measures are generally the detailed and technical methods of controlling the mentioned scopes. For example, operating system hardening measures are generally covered by ISO 27001 in access control matters. This scope in ICSG is a detailed and rule-based checklist specifically processed for each operating system. However, more detailed and technical controls, including ISO 27001, are not found in NIST IR 7621 and TCA's IT audit.

On the other hand, similarly, database hardening methods are generally covered in the operations security scope of ISO 27001. However, a detailed set of rules is not found in ISO 27001, NIST IR 7621, and TCA's IT audit in the same way.

Finally, the subcategories of server hardening measures are web server hardening measures and virtualization server Hardening Measures. Although ISO 27001 insufficiently mentioned the specified scope, the scope is available in NIST IR 7621, and TCA's IT audit.

Table 3.3 : Scope comparison of ISO 27001, NIST IR 7621, TCA's IT Audit, and ICSG with given grading criteria in Table 3.2

Scope	ISO 27001	NIST IR 7621	IT Audit	ICSG
Network and System Security	5	2	4	5
Application and Data Security	5	4	5	5
Removable Devices and Media Security	5	1	1	5
Internet of Things (IoT) Security	5	1	1	5
Personnel Security	5	3	4	5
Physical Environment Security	5	2	4	5
Personal Data Security	5	3	4	5
Instant Messaging Security	5	1	1	5
Cloud Security	5	1	1	5
Security of Crypto Applications	5	1	1	5
Critical Infrastructure Security	5	2	3	5
Supply Chain Security	5	1	1	5
Operating System Hardening	2	1	1	5
Database Hardening	2	1	1	5
Server Hardening	2	1	1	5

4. CYBERSECURITY THREATS TARGETING SMEs AND STRATEGIC SCOPE ANALYSES

Small enterprises lack awareness and readiness, often lacking a structured IT department in comparison to larger organizations [3]. Hence, it is inevitable that small and medium-sized enterprises (SMEs) face a high frequency of cyber attacks. In reports tailored for SMEs, various types of attacks posing threats to these enterprises are delineated. According to ENISA's report, SMEs are vulnerable to phishing, web-based attacks, malware, malicious insider activities, denial of service, social engineering, and compromised/stolen device attacks [13]. Additionally, in reports issued by the Austrian government and the Australian Cyber Security Centre, attacks threatening SMEs are outlined as scam messages, email attacks, and malicious software [42]. In this section, the incident rates and types of attacks faced by SMEs will be evaluated with statistical amounts from three distinct perspectives.

In the context of Turkey, as a developing country, approximately 28.5% of businesses experience exposure to at least one security breach in 2022 [6]. In the conducted research, the mentioned incidents have been classified as follows: (i) 18% is inaccessibility of information and communication technology services due to hardware and software failures, (ii) 8.8% is loss of data due to hardware and software failures, (iii) 6.5% is inaccessibility of information and communication technologies services due to external attacks, (iv) 6.5% is loss of data due to malware or unauthorized access, (v) 3.9% is data privacy incidents due to intrusions, fraud, phishing attacks and intentional acts of employees of the enterprise, (vi) 3.3% is disclosure of confidential data due to unconscious/unintentional actions of employees [6].

According to information found on the cybersecurity page of the report released by the United States on SMEs, similarly, 29% of SMEs were the target of a cyberattack in 2021 in the US. In line with the above study; 39% of victims have experienced a service interruption, 25% of them were falsely sent private information from their

domains, 18% of them faced website blocks, 11% of them experienced stolen sensitive information and data, 4% of them lost access to business banking accounts to hackers, 9% of them faced ransomware attacks by hackers and 5% of them faced other attacks and impacts [43].

As evident in Verizon's regularly published Data Breach Investigations Report, the size of a business has not altered the likelihood of becoming a target. Furthermore, the rates and types of attacks have emerged proportionally correlated with each other. In this report, businesses are categorized based on their industry, size, region, and the times they are subjected to attacks. It is observed that these figures are increasing in another survey from March 2022 that consider incidents globally. 61% of SMEs were the target of a cyberattack. Most common attack types are ordered as; malware is 18%, followed by phishing by 17%, data breaches are 16%, website hacking is 15%, DDoS attacks are 12%, and ransomware is 10%, [7].

4.1 Mapping Attacks to Scopes

The attacks encountered during the matching phase, following the three different perspectives and the report, have been grouped. Firstly, the data from the developing country which is "unavailability of information and communication technology services due to hardware and software failures" has been consolidated as the "service interruption" category. Similarly, "inaccessibility of information and communication technologies services due to external attack" is considered as a "website block". Loss of data due to hardware and software failures is categorized as a "data breach," while data loss due to malware or unauthorized access is classified as "malware." Data privacy incidents resulting from unauthorized entries, fraud, phishing attacks, and intentional acts of enterprise employees are grouped as "unauthorized access," and the disclosure of confidential data due to the unconscious/intentional actions of employees is considered a "PII leakage" attack.

On the other hand, the item stating "they were falsely sent private information from their domains" is classified as "PII leakage", the item mentioning "stolen sensitive information and data" is categorized as "data breach", and the statement indicating "lost access to business banking accounts to hackers" is labeled as "unauthorized

access". Finally, while retaining the data from the DBDIR report as is, the denial of service attack type has been classified under the "service interruption" category.

In order to find the collective percentages of categorized attack types, the averages of the three given sources [6], [43], and [7] were taken, revealing the most encountered attack types for small and medium-sized enterprises. The common incidents for SMEs can be ordered by their likelihood. Among these types are: 23.03% for service interruption, 13.17% for website block, 12.97% for phishing, 11.93% for data breach, 10.73% for PII leakage, 8.17% for malware, 6.33% for ransomware, and 2.63% for unauthorized access. From this point forward, the specified attack types will be elucidated, and an analysis will be conducted to determine which cybersecurity scope these types can be associated with. The mappings conducted are visualized in Figure 4.1.

4.1.1 Service interruption

Service interruption attacks involve overwhelming the target device by generating a high volume of requests within a short time period or by sending requests that the target device is unable to handle. Service interruption can occur due to factors such as hardware or software failures, power outages, security incidents, and network congestion [44]. In this context, service interruption issues are connected to *network and system security* and *physical environment security*. Strengthening these scopes could prevent the problems caused by this issue.

4.1.2 Website block

The website block type is also a form of attack that can lead to service interruptions. However, it should be noted that attacks initiated by an attacker through a website are distinctly evaluated, as indicated in various sources [6], [43], and [7]. For this reason, the website block is defined separately. Website block/ hacking attacks refer to incidents where attackers, through technical means such as SQL injection, phishing, cross-site scripting, and brute force attacks, compromise the security of an organization's websites [45]. These attacks can lead to consequences such as the loss of website access or the destruction, alteration, or theft of information within the website.

In this case, measures of network and system security scope could eliminate the risk of aforementioned attacks.

4.1.3 Phishing

Phishing attacks are a type of threat where attackers attempt to obtain information directly from businesses through methods such as email, instant messaging, or other electronic communication channels [46]. Mitigating such attacks may require personnel training or advanced software configurations to filter phishing messages [46]. In cases where SMEs may not have the capability to use advanced software, this type of attack can be directly associated with *personnel security* measures, enabling preventive measures to be implemented.

4.1.4 Data breach

A data breach is the intentional or unintentional disclosure of confidential information to unauthorized individuals or entities. Data breaches may arise from diverse causes, encompassing cyberattacks, insider threats, and human errors [47]. In the same study, these reasons were elaborated, and the causes of data breaches were categorized as phishing, insider threats, malware, inadequate industrial solutions, the exponential growth of data, and encryption failure. The measures to address this issue include implementing robust access controls and permissions, establishing clear data breach response plans and procedures, utilizing strong encryption methods to protect data, conducting regular employee training and awareness, and utilizing intrusion detection and prevention systems [47]. Since phishing attacks and PII leakage issues are specifically addressed separately, it is anticipated that problems related to data breaches could be prevented within the scope of application and data security and security of personal data.

4.1.5 Personally identifiable information (PII) leakage

PII refers to information that could identify an individual, either on its own or when combined with other linkable information. The problem of disclosing confidential data due to the unconscious or unintentional actions of employees is also referred to as PII

leakage. PII leakage occurs when this sensitive information is accessed, shared, or obtained by unauthorized parties [48]. This issue is directly associated with privacy and has been identified as a matter that requires legal protection in many regions. The measures taken to address this issue include implementing strong privacy settings and controls, informing and educating users about the significance of privacy and the potential risks associated with sharing sensitive information, implementing strict access controls and authentication mechanisms, and establishing clear policies and guidelines [48]. Hence, the PII leakage issue is aligned with the personnel security and security of personal data scopes.

4.1.6 Malware

Malware is software created with the intention of disrupting, causing damage to, or gaining unauthorized access to computer systems or networks [49]. There are various types of malware such as viruses, worms, Trojans, ransomware, and spyware. Although malware poses a significant threat, precautionary measures to mitigate its impact include:(i) keeping the software and operating systems up to date, (ii) using reputable antivirus and anti-malware software, (iii) enabling firewalls and using network security measures, (iv) regularly backup important data, (v) using email filters and spam blockers, (vi) educating users about safe browsing habits, and (vii) employing intrusion detection and prevention systems [49]. Most of the preventive measures fall within the scope of network and system security. Therefore, this issue is aligned with the coverage of network and system security.

4.1.7 Ransomware

Ransomware, a form of malicious software, infects computers and encrypts their content, demanding ransom for decryption. Usually, this attack spreads through phishing emails and malicious attachments. The cost of ransomware attacks exceeds $1 million in 2023 [50]. Regularly backing up important data, keeping software and operating systems up to date, using reputable antivirus and anti-malware software, educating users, and restricting user privileges could significantly mitigate the impact

of ransomware attacks [50]. Hence, ransomware is also mapped to the scope, *network and system security*.

4.1.8 Unauthorized access

Unauthorized access is when someone, an attacker, gains or tries to gain entry into a computer system, network, or account without proper authorization. This could involve bypassing security measures or taking advantage of weaknesses in order to access sensitive information or carry out unauthorized activities. Unauthorized access can take place through different methods like hacking, cracking passwords, manipulating others through social engineering, and exploiting software vulnerabilities. Various strategies such as implementing strong authentication procedures, using access controls and encryption, utilizing intrusion detection systems and firewalls, regularly updating and patching software, as well as conducting routine security audits are employed to prevent unauthorized access [51]. Given that preventive measures beyond network and system security, such as application and data security measures and strategies, can address this type of attack, this attack category is associated with the coverage of *application and data security*.

4.2 The Attack Surfaces of the Identified Scopes

According to Figure 4.1, Service interruption, malware, and ransomware are mapped to network system security. While personnel security is mapped by phishing and PII leakage attacks, security of personal data, security of PII, is mapped by PII leakage and data breach attacks. Also, application and data security measures could prevent data breaches and unauthorized access attacks. Finally, service interruption attacks have also been linked to physical environment security. Considering the rates of attacks, the attack surfaces of the scopes can be listed as follows:

- %37.64 for Network and System Security
- %10.81 for Application and Data Security
- %17.60 for Personnel Security

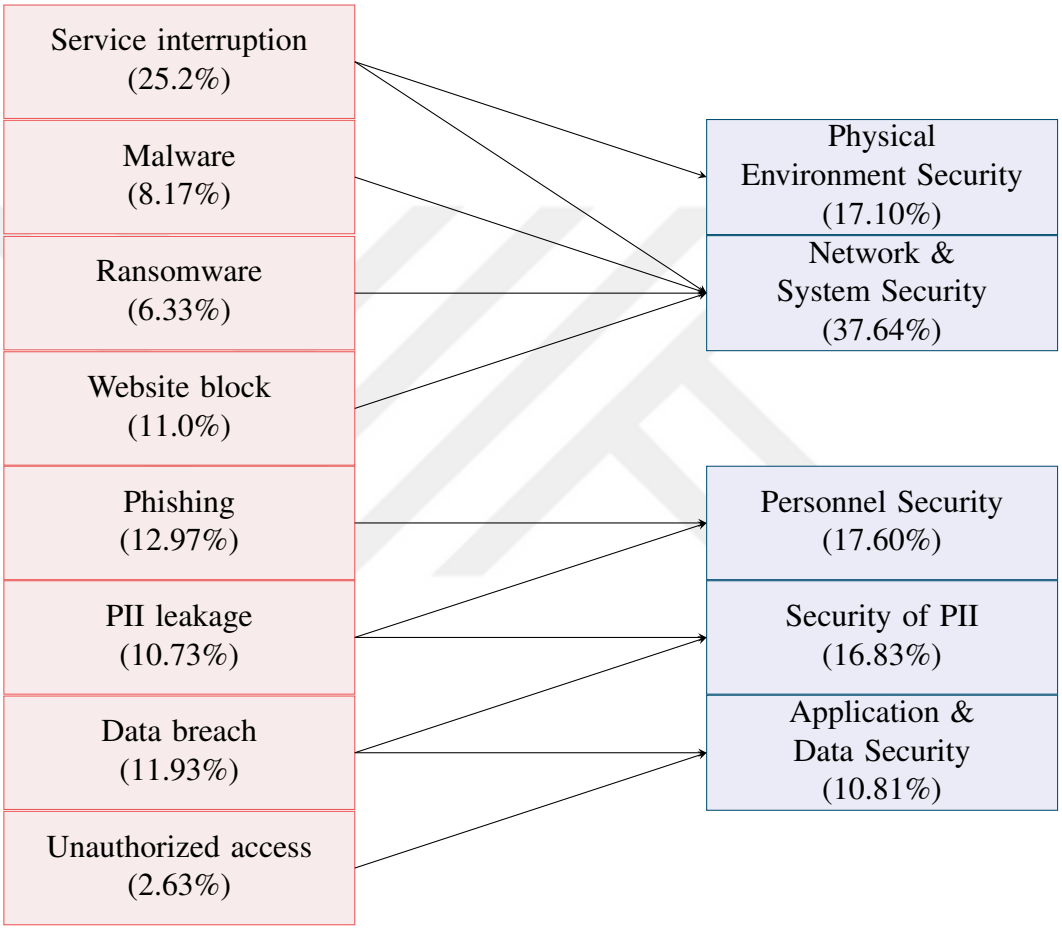

Figure 4.1 : Mapping of most common problems to effective certification scopes

- %17.10 for Physical Environment Security
- %16.83 for Security of Personal Data

5. PRIORITIZATION EXPERIMENTS AND RESULTS

In this section, information about the prioritization of the aforementioned framework setup and evaluation metrics is given. During the prioritization of the mentioned structures, a ranking system is employed to assign scores. The score of rank depends on three parameters which are frequency, weight, and easiness.

5.1 Easiness Value

The easiness value is a metric for SMEs that denotes the ease of use with which assigned scope items for them. The easiness factor is low for scopes that are challenging for an SME to accomplish due to various reasons (technical, financial, etc.). The easiness value of implementation is sketched depending on measures of complexity, financial cost, time frame, resources, and compliance factors. This value has been elaborated separately for each scope, and the final results are presented in Table A.1. However, the basic aspects of assigning easiness value are defined. The easiness value ranges from 0.2 to 1 with intervals of 0.2.

Due to the complexity of configuration and management, network and system security is hard to implement which might require expertise. Similarly, IoT devices are often vulnerable to cyber-attacks and could be difficult to keep up to date, monitor and manage. Cloud security, like IoT, is one of the new technologies. It is considered difficult due to the challenges of having sufficient resources and experienced personnel. It is important that crypto applications are properly configured and managed. The scope of security of crypto applications is noted to be challenging due to its intricate nature, requiring time-consuming configuration and management processes, necessitating expertise in the field. Additionally, the critical infrastructure security scope faces challenges in applicability and management due to the complexity and ever-changing nature of cyber threats within this scope. The mentioned four scopes have the lowest easiness values, each having a value of 0.2.

The hardening measures scopes have an easiness value of 0.4. This is attributed to the fact that operating system hardening processes require careful planning and implementation. If the specified technical measures are executed incorrectly, they can lead to system issues and security vulnerabilities. Knowledgeable personnel should be given sufficient time during the planning and implementation phases. Database hardening affects data access and availability, while server hardening processes impact system performance. Therefore, technical controls in these scopes should be carried out by knowledgeable and experienced individuals. It is also important to consider that these controls may be time and cost-intensive. Also, application security should be integrated into software development processes and carefully managed at every stage of these processes. Key aspects of application security, such as session management, authentication, and authorization, are handled within this scope. Additionally, it encompasses complex controls like malicious process prevention and the security of external system integrations. Compliance processes should also be well-planned. Due to these reasons, the difficulty level is assigned as 0.4.

Complying with personal data protection regulations could be complex, and safeguarding sensitive information could be challenging. Additionally, the correct implementation of encryption and security measures is crucial. The use of uncontrolled instant messaging could pose a security risk. However, it is believed that with a knowledgeable team, compliance could be achieved in a reasonable amount of time. Due to these reasons, the difficulty level is assigned as 0.6.

Removable devices and media security scope is related to the implementation of information security policies and prevention of unauthorized use of portable devices. It is one of the easier scopes to implement, requiring less workforce and time compared to other scopes, and its easiness of compliance. Additionally, personnel security involves easy awareness and training measures. Implementing the rules of this scope is easier compared to other scopes. Similarly, physical security measures are cost-effective, and management and implementation are more easily achievable compared to other scopes. Finally, the new developments and supply scope incurs medium costs due to rapid technological changes and the global supply chain. However, with relatively easy

compliance processes and scope difficulty, it is considered easy. These four scopes are categorized as easy, having an easiness value of 1.

5.2 Attack Frequency

Additionally, the attack frequency is derived from the analysis of the mapping of the attack scope items applied in Section 4. Examining the values in the specified figure, the attack frequencies for the network and system security scope, application and data security scope, personnel security, and physical environment security scopes are determined as 0.37, 0.10, 0.17, 0.17, and 0.16, respectively. Also, the attack frequencies for the other scopes are assumed to be 0.001.

5.3 Weight Value

The weight of each scope matter is based on the evaluation of risk and potential damages. The weight value could be determined by optimizing the product of the risk understood from the frequency of attacks and the potential damage values. The potential damage values are explained as follows:

- **Security of Personal Data:** Given the potential fines from regulatory bodies and the loss of customer trust, it is assigned a value of 1.
- **Network and System Security and Application and Data Security:** Both are considered as having critical information that could disrupt business continuity and require technical expertise and time for recovery, hence assigned a value of 1 each.
- **Personnel Security:** Due to vulnerabilities that could indirectly lead to attacks and cause financial losses, it is assigned a value of 0.8.
- **Physical Environment Security:** Considering the potential financial damage and disruption of operations due to physical damage to devices, it is assigned a value of 0.6.

The hardening scopes, including Operating System Hardening, Database Hardening, and Server Hardening, are protected by other scopes. However, compromising the confidentiality, integrity, and availability of the critical information they contain harms

the system. Similarly, cloud security and critical infrastructure security might have critical information that could disrupt the continuity of business. Therefore, the potential damage of mentioned scopes is determined to be 0.5.

The potential damage values for the "Removable Devices and Media Security" and "Internet of Things (IoT) Security" scopes are assessed as 0.2. This is due to the nature of these scopes, which do not carry critical information and are easily replaceable.

The process of finding the optimized weight with the specified values is illustrated in Table 5.1.

5.4 Evaluating Result

The product of these three main parameters is used to obtain a degree for each scope. The sum of all scope degrees determines the overall framework degree. The formulas mentioned are as follows:

The scope measure is defined as in Equation 5.1.

$$M_s = F \times W \times E \tag{5.1}$$

The total rank for security measures is defined as in Equation 5.2.

$$Rank = \sum M \tag{5.2}$$

During the rating stage, the considerations, all security frameworks are assumed to be reliable and resilient to the types of attacks mentioned, have been taken into account. Additionally, based on this information, the best and optimal result emerges with the result where the easiness value is the highest for each scope. The best result is calculated to be 0.234934971. The optimal value, which can be assigned by examining normalized variables, being 0.23 is the result of a trade-off between easiness of implementation and effectiveness. In the ideal scenario, it should be noted that the easiest and most effective method would have a value of 1, whereas the practical presentation has a value of 0.23.

Table 5.1 : Finding weight values for scopes

Scope	Risk	Damage	Weight	Optimized Weight
Network and System Security	0.37	1	0.37	1
Application and Data Security	0.10	1	0.10	0.3
Removable Devices and Media Security	0.01	0.2	0.002	0.005
Internet of Things (IoT) Security	0.01	0.2	0.002	0.005
Personnel Security	0.17	0.8	0.13	0.37
Physical Environment Security	0.18	0.6	0.11	0.30
Security of Personal Data	0.16	1	0.16	0.45
Instant Messaging Security	0.01	0.2	0.002	0.005
Cloud Security	0.01	0.5	0.005	0.01
Security of Crypto Applications	0.01	0.3	0.003	0.01
Critical Infrastructure Security	0.01	0.5	0.005	0.01
New Developments and Supply	0.01	0.4	0.004	0.01
Operating System Hardening	0.01	0.5	0.005	0.01
Database Hardening	0.01	0.5	0.005	0.01
Server Hardening	0.01	0.5	0.005	0.01

For the existing frameworks, when the rank formula is applied, the result can be shown in Table 5.1. Each framework's easiness is calculated by the formula:

$$Easiness/ScopeGrade \tag{5.3}$$

The ISO 27001 and ICSG, which have been noted to have a wide scope in Table 3.3, have been concluded as not suitable for SMEs due to implementation difficulties in

Table 5.2 : Frequency, Weight and Easiness Values for Existing Scopes

Scope	Frequency	Weight	Easiness
Network and System Security	0.370	1.00	0.2
Application and Data Security	0.106	0.29	0.4
Removable Devices and Media Security	0.001	0.005	1
Internet of Things (IoT) Security	0.001	0.005	0.2
Personnel Security	0.172	0.37	1
Physical Environment Security	0.185	0.30	1
Personal Data Security	0.165	0.45	0.6
Instant Messaging Security	0.001	0.005	0.6
Cloud Security	0.001	0.01	0.2
Security of Crypto Applications	0.001	0.01	0.2
Critical Infrastructure Security	0.001	0.01	0.2
Supply Chain Security	0.001	0.01	1
Operating System Hardening	0.001	0.01	0.4
Database Hardening	0.001	0.01	0.4
Server Hardening	0.001	0.01	0.4

Table 5.2. Similarly, it has been observed that the IT audit has received a low rating due to implementation difficulties. As expected, depending on Table 5.3, despite NIST IR 7621's limited comprehensive scope, it has received a high rating and approached an optimal result by 42% due to its compliance with SMEs. Therefore, the ranks are listed as follows, from largest to smallest are NIST IR 7621, TCA's IT audit, ISO 27001, and ICSG. It is inevitable that NIST IR 7621, which is intended for SMEs, is the most reasonable choice.

Table 5.3 : Ranks of aforementioned frameworks

Grade	Rank	Practical Boundary
ISO 27001	0.04994	%20.001
NIST IR 7621	0.1036	%41.55
TCA's IT audit	0.0618	%24.76
ICSG	0,04993	%20

6. INSIGHTS

In this section, the preference of the aforementioned frameworks mentioned for SMEs is assessed in terms of usability. Additionally, a five-point recommendation list is provided, outlining how SMEs could easily achieve sufficient security measures.

6.1 Preference of the Aforementioned Frameworks

An organization could favor any of the security frameworks. Our assumptions on the rating of these frameworks depend on the perspective of SMEs. The SMEs are assumed to lack technical knowledge, IT experience, and limited budgets. Additionally, our comprehensive observation of each of the frameworks reveals the following paragraphs.

If the business gains benefits after the certification, ISO 27001 should be chosen, depending on the certifiable criteria of Table 3.1. ISO 27001 is the most comprehensive certifiable framework among the four frameworks. It has a detailed certification structure and a wide scope that contains a wide spectrum of diverse security aspects. However, the formal certification path is an additional cost for small to medium-sized businesses. It is observed that technically inexperienced SMEs could suffer from adapting the framework to their system.

Also, if the SME thoroughly understood its security requirements, NIST IR 7621 could be preferred. NIST IR includes fundamentals of the ISMS framework for SMEs. Note that, NIST IR 7621 is a subset of ISO 27001 and ICSG. It has limited coverage depending on the other two. This situation is expected and in line with the targeted audience of NIST IR 7621. As predicted, it receives the highest grade regarding our rankings.

TCA's IT audit should be categorized properly for the administrated aspect. There is a limited source of information management security since it is designed mostly for financial and administrated concerns. TCA's audit is designed for auditors. The effects

of the technical language might increase the cost since it requires IT. Even though public institutions are not our target, the framework is considered suitable for them.

ICSG took advantage of ISO 27001's sources and added local and regional matters to it. According to this, it would be appropriate for medium-level and bigger enterprises and public institutions in Turkey to comply with this certificate since this framework is suitable for obtaining legal guarantees. The rank of ICSG is slightly less than the ISO 27001 even though it has a wider coverage. This is due to the difficulty of adopting all of the security strategies. Therefore, the guide is also not suitable for SMEs.

6.2 Sufficient Security Measures

However, upon reviewing these rankings, it has been contemplated that cost-effective security measures can also be provided. This is the most cost-effective way for SMEs for sufficient security.

- Finding vulnerable assets by creating an asset inventory is crucial. The assets are defined as IT equipment.
- IT equipment must be protected and isolated.
- Otherwise, it should be ensured about proper handling of data backup or hardware and software supply chain.
- Regular updates and malware protection are effective; otherwise, SMEs can access their lost or unreachable data through backups. Backup is the most effective quick recovery method used for network and security system problems.
- Employees could be trained to identify social engineering techniques and PII leakage attempts. Knowledge about password security should be gained. Also, the importance of screen locking and information sharing should be explained and awareness should be raised during the recruitment and departure process. Employees should ensure that no information is left when selling or disposing of any device. On the other hand, some attacks like ransomware could be injected even if the software is updated and malware protection is available. These attack types could be injected by email, files, or dangerous websites. As a result of that,

SMEs should be aware of dangerous emails or files. Employees of SMEs should not open malicious emails, files, and websites for malware, phishing, ransomware, or service interruptions.

On the other hand, the thesis gives three pieces of advice to enhance SMEs' cyber security without any outsourced consultancy. These devices are compatible for self-assessment. This advice is believed to restrict a great number of attacks or an easy path for recovery. Our proposed advice for SMEs, which are expected to be implemented by them, can be explained as follows: The first item in these recommendations emphasizes the importance of creating an inventory list, as highlighted by many security frameworks. The second of these advice, which is ensuring the security of IT equipment, can address a portion of the service interruption issue within the physical security, amounting to 18.41%. Otherwise, as a third matter, the backups in use serve as a recovery for both physical and network-related data issues. Making this step is not only effective in preventing the most common problem but also facilitating the recovery process. Besides, the fourth advice which recommends regular updates and malware protection is aimed to restrict service interruptions caused by software failures, malware, website block, and ransomware incidents. These prevented attacks account for 37.05% of the most common attack types. Following this step reduces the risk of encountering the specified network and system security attacks. Otherwise, the damage could still mitigated by using backups. The final recommendation aimed at employee security is provided to prevent phishing attacks, intentional as well as unintentional PII leakage errors, and ransomware attacks which cannot be addressed through updates or antivirus applications. Inventories need to be specified in the first recommendation, and employees should be trained accordingly to complete this step. The attack types stemming from personnel security issues constitute 17% of the encountered attack types. Therefore, ensuring this step is just as important as the others. As a result of these matters, SMEs could cover up to 72% of attacks only by following these five recommendations.

Even though the mapping includes a limited number of practically applicable scopes, some of them cover a wider percentage of common problems. Therefore, a set of easy

and effective advice could be formed. Based on the incident frequencies shown on surveys, it is estimated that up to 72% of the problems could be covered to an extent by the countermeasures proposed by the thesis.

7. CONCLUSION

As large enterprises bolster their security measures through increased financial resources, the surge in cyber threats targeting SMEs becomes inevitable. Consequently, the role of information security management takes on paramount significance for SMEs. In navigating their cybersecurity landscape, SMEs must judiciously select a security framework tailored to their objectives, financial capacities, and anticipated benefits. Since, SMEs encounter difficulties in achieving sufficient security standards due to challenges such as a shortage of qualified candidates in the recruitment process, regulatory fines, and penalties, insufficient qualifications in the relevant field, lack of relevant work experience, and high wage expectations, information can be conveyed through this thesis. The initial goal of the thesis was to create two tables that would assist small and SMEs in the cybersecurity measures path. For this purpose, four different frameworks were analyzed and compared. Common and distinct features were identified and interpreted from the perspective of SMEs. Additionally, common attack types, potential measures, and associated scopes are informative for SMEs to find the appropriate framework to fortify defenses and mitigate liability risks. However, for more effective guidance, four distinct frameworks have been elucidated, their importance highlighted through a nuanced prioritization based on scope and frequency values. The comparative analysis of these frameworks has yielded a compliance ranking, calculated by factoring in scope, attack frequency, and weighted values. Thus, the frameworks evaluated from the perspective of SMEs are ranked as follows: NIST IR 7621, TCA's IT audit, ISO 27001, and ICSG. The hierarchical classification of scope expansiveness, tailored to the exigencies of SMEs, is delineated as follows: ICSG, ISO 27001, TCA's IT Audit, and NIST IR7621. In the context of complexity, the hierarchical arrangement of frameworks available for selection by SMEs is delineated as follows: NIST IR 7621, ISO 27001, ICSG, and TCA's IT Audit. Moreover, in terms of the benefits that certification or established frameworks could

bring to enterprises due to reliability and customer trust, the ranking is as follows: ISO 27001, ICSG, TCA's IT Audit, and NIST IR7621.

In addition, another goal of the thesis, which is cost-effective security measures, has been determined based on attack analyses. As a result of the analyses, the security measures for the network and system security scope, application and data security scope, personnel security, and physical environment security scopes have been emphasized as the necessary areas for implementing security measures. Therefore, the thesis provided recommendations for cost-effective security measures within these scopes, aiming to enhance SMEs' resilience against fundamental cybersecurity challenges and minimize potential risks when implemented. Consequently, practical and cost-effective recommendations that have been proffered to address critical incidents cover a substantial 72% of the most prevalent attacks experienced by SMEs.

REFERENCES

[1] **Worldbank** (2021). *Small And Medium Enterprises (SMES) Finance*, https://www.worldbank.org/en/topic/smefinance.

[2] **TÜİK Haber Bülteni** (2012). Küçük ve Orta Büyüklükteki Girişim İstatistikleri, **Technical Report**.

[3] **Gordon, M.S.** (2018). *Economic and national security effects of cyber attacks against small business communities*, Utica College.

[4] **Tsochev, G.**, **Trifonov, R.**, **Nakov, O.**, **Manolov, S. and Pavlova, G.** (2020). Cyber security: Threats and Challenges, *2020 International Conference Automatics and Informatics (ICAI)*, IEEE, pp.1–6.

[5] **Schuh, G.**, **Hicking, J.**, **Engländer, J.**, **Zeller, V. and Perau, M.** (2020). Helping companies to evaluate their status quo in information security with a serious gaming-based economical quantification approach, *Procedia CIRP*, *93*, 587–592.

[6] **TÜİK** (2022). *Girişimlerde Bilişim Teknolojileri Kullanım Araştırması*, https://data.tuik.gov.tr/Bulten/Index?p=Girisimlerde-Bilisim-Teknolojileri-Kullanim-Arastirmasi-2022-45585.

[7] **Verizon** (2023). *2023 Data Breach Investigations Report*, https://www.verizon.com/business/resources/reports/dbir/.

[8] **Paulsen, C. and Toth, P.** (2016). Small business information security: The fundamentals, **Technical Report**, National Institute of Standards and Technology.

[9] **Falch, M.**, **Olesen, H.**, **Skouby, K.E.**, **Tadayoni, R. and Williams, I.** (2023). Cybersecurity Strategies for SMEs in the Nordic Baltic Region, *Journal of Cyber Security and Mobility*, *11*(6), 727–754.

[10] **Gaitero, D.**, **Genero, M. and Piattini, M.** (2021). System quality and security certification in seven weeks: A multi-case study in Spanish SMEs, *Journal of Systems and Software*, *178*, 110960.

[11] **Ključnikov, A.**, **Mura, L. and Sklenár, D.** (2019). Information security management in SMEs: factors of success, *Entrepreneurship and Sustainability Issues*, *6*(4), 2081.

[12] **Ncubukezi, T.**, **Mwansa, L. and Rocaries, F.** (2020). A review of the current cyber hygiene in small and medium-sized businesses, *2020 15th International Conference for Internet Technology and Secured Transactions (ICITST)*, IEEE, pp.1–6.

[13] **Sarri, A.**, **Paggio, V. and Bafoutsou, G.** (2021). CYBERSECURITY FOR SMES-Challenges and Recommendations, *European Union Agency for Cybersecurity, ENISA, Heraklion, Greece*.

[14] **Dewanto, M.R.P.**, **Oktavia, T.**, **Sundaram, D.**, **Archana, K.**, **Vanithamani, D.**, **Bakti, D.W.**, **Mulyana, D.**, **Baharuddin, A.R.**, **Sembiring, M.A.R.**, **Zhabayev, Y.** *et al.* (2022). Comparative Study of Information Security Evaluation Models for Indonesia Government, *Journal of Theoretical and Applied Information Technology*, *100*(04).

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

[16] **Roy, P.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)*, IEEE, pp.1–3.

[17] **Alshar'e, M.** (2023). Cyber Security Framework Selection: Comparison of NIST and ISO27001, *Applied computing Journal*.

[18] **Sulistyowati, D.**, **Handayani, F. and Suryanto, Y.** (2020). Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss, *JOIV: International Journal on Informatics Visualization*, *4*(4), 225–230.

[19] **Benslimane, Y.**, **Yang, Z. and Bahli, B.** (2016). Information security between standards, certifications and technologies: An empirical study, *2016 International Conference on Information Science and Security (ICISS)*, IEEE, pp.1–5.

[20] **Teufel, S.**, **Teufel, B.**, **Aldabbas, M. and Nguyen, M.** (2020). Cyber security canvas for SMEs, *Information and Cyber Security: 19th International Conference, ISSA 2020, Pretoria, South Africa, August 25–26, 2020, Revised Selected Papers 19*, Springer, pp.20–33.

[21] **Alharbi, F.**, **Alsulami, M.**, **Al-Solami, A.**, **Al-Otaibi, Y.**, **Al-Osimi, M.**, **Al-Qanor, F. and Al-Otaibi, K.** (2021). The impact of cybersecurity practices on cyberattack damage: The perspective of small enterprises in Saudi Arabia, *Sensors*, *21*(20), 6901.

[22] **Ashley, C. and Preiksaitis, M.** (2022). Strategic Cybersecurity Risk Management Practices for Information in Small and Medium Enterprises, *Business Management Research and Applications: A Cross-Disciplinary Journal*, *1*(2), 109–157.

[23] **Armenia, S.**, **Angelini, M.**, **Nonino, F.**, **Palombi, G. and Schlitzer, M.F.** (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs, *Decision Support Systems*, *147*, 113580.

[24] **Talu, S.** (2020). Strategic Measures in Improving Cybersecurity Management in Micro and Small Enterprises, *2nd International Scientific and Practical Conference on Digital Economy (ISCDE 2020)*, Atlantis Press, pp.522–528.

[25] **García, J.E.**, **Encinas, L.H. and Domínguez, A.P.** (2021). A Comprehensive Security Framework Proposal to Contribute to Sustainability, *Sustainability*.

[26] **Alsmadi, I.** (2020). Training, Education, and Awareness, 229–239.

[27] **Culot, G.**, **Nassimbeni, G.**, **Podrecca, M. and Sartor, M.** (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda, *The TQM Journal*.

[28] **Malatji, M.** (2023). Management of enterprise cyber security: A review of ISO/IEC 27001: 2022, *2023 International Conference On Cyber Management And Engineering (CyMaEn)*, IEEE, pp.117–122.

[29] **Taherdoost, H.** (2022). Understanding Cybersecurity Frameworks and Information Security Standards—a Review and Comprehensive Overview, *Electronics*, *11*(14), 2181.

[30] **Calder, A.** (2013). *ISO27001/ISO27002: A pocket guide*, IT Governance Publishing.

[31] **Middleton, T.T.** (2022). *Effective Cybersecurity Risk Management Policies for the Residential Real Estate Industry*, Capella University.

[32] **Jian-bin, L.** (2008). ISMS Concept Model Exploration, *Computer Engineering*.

[33] **Kosutic, D.** (2023). *Mandatory ISO 27001 documents 2022 revision: Get The full list*, `https://advisera.com/27001academy/knowledgebase/list-of-mandatory-documents-required-by-iso-27001-revision/`.

[34] **NIST** (2018). *New NIST Guide Helps Small Businesses Improve Cybersecurity*, `https://www.nist.gov/news-events/news/2016/11/new-nist-guide-helps-small-businesses-improve-cybersecurity`.

[35] **Alshboul, Y. and Streff, K.** (2015). Analyzing information security model for small-medium sized businesses.

[36] **Özkul, D.** (2013). *Bilişim Sistemleri Denetimi Rehberi*.

[37] **Yıldız, Ö.R.** (2007). Bilişim sistemleri denetimi ve Sayıştay, *Sayıştay Dergisi*, (65), 173–185.

[38] **Kayrak, M.** (2013). Bilişim Teknolojileri Yönetişimi, *Sayıştay Dergisi*, (91), 57–76.

[39] **ASOSAI** (2003). IT Audit Guidelines, *ASOSAI Research Project*.

[40] **Türkiye Cumhuriyeti Cumhurbaşkanlığı - Dijital Dönüşüm Ofisi** (2020). *Bilgi ve İletişim Güvenliği Rehberi*.

[41] **Özbilger, H.**, **Sarıyar, B. and Ertürk, A.** (2023). Bilgi ve İletişim Güvenliği Rehberinin Uygulanması ve Denetimlerine Yönelik İyileştirme Önerileri, *Bilgi Teknolojileri ve İletişim Dergisi*, *1*(1 (Eylül 2023)), 1–41.

[42] **Government, A. and ACSC** (2023). Small business cyber security guide, **Technical Report**, Australian Cyber Security Centre, `https://www.cyber.gov.au/sites/default/files/2023-07/acsc_small_business_cyber_security_guide.pdf`.

[43] **CISCO and NSBA** (2021). 2021 U.S. Small Business Recovery and Technology Report, **Technical Report**, National Small Business Association, `https://www.nsba.biz/_files/ugd/fec11a_eb986c9607d34c72a83ee6b0a490b1dd.pdf`.

[44] (2019). *Service interruption reporting*.

[45] **Shaukat, K.**, **Aqeel, S.**, **Zafar, N. and Kayani, Z.** (2017). Software Hacking, Protection and Testing, *Transylvanian Review*, *1*.

[46] **MITRE ATT&CK** (2023). Phishing for Information, `https://attack.mitre.org/techniques/T1598/`.

[47] **Das, P.K.** (2023). An Insight into Data Breaches: Challenges and Prevention, *Soc. Sci*, *3*(1), 1–8.

[48] **Krishnamurthy, B. and Wills, C.** (2009). On the leakage of personally identifiable information via online social networks, *Comput. Commun. Rev.*, *40*, 112–117.

[49] **Alenezi, M.N.**, **Alabdulrazzaq, H.**, **Alshaher, A.A. and Alkharang, M.M.** (2020). Evolution of malware threats and techniques: A review, *International Journal of Communication Networks and Information Security*, *12*(3), 326–337.

[50] **Hyslip, T.S. and Burruss, G.W.** (2023). 5. Ransomware, *Handbook on Crime and Technology*, 86.

[51] **Mitchell, R.S.** (2023). *Methods and systems for detecting unauthorized access by sending a request to one or more peer contacts*, uS Patent 11,616,774.

APPENDICES

APPENDIX A : Easiness value evaluation map

APPENDIX A : Easiness value evaluation map

Table A.1 : The easiness value of each scope

Scope	Complexity	Cost	Time-frame	Resources	Compliance	Total	Easiness Value
Network and System Security	high	high	high	high	high	high	0.2
Application and Data Security	medium	high	high	medium	high	medium-high	0.4
Removable Devices and Media Security	low	medium	low	medium	low	low	1
Internet of Things (IoT) Security	medium	high	medium	high	high	high	0.2
Personnel Security	low	medium-low	low	low	low	low	1
Physical Environment Security	low	medium-low	low	low	low	low	1
Security of Personal Data	high	medium-high	medium	high	high	medium-high	0.6
Instant Messaging Security	medium	medium	medium	medium	medium	medium	0.6
Cloud Security	medium	high	high	high	high	high	0.2
Security of Crypto Applications	high	high	high	high	high	high	0.2
Critical Infrastructure Security	high	high	high	high	high	high	0.2
New Developments and Supply	low	medium	low	low	low	low	1
Operating System Hardening	medium	high	high	high	medium	medium-high	0.4
Database Hardening	high	high	high	high	medium	medium-high	0.4
Server Hardening	high	high	high	high	medium	medium-high	0.4

CURRICULUM VITAE

Name SURNAME: Gizemnur TAŞKIN

EDUCATION:

- **B.Sc.:** 2020, Istanbul Technical University, Faculty of Computer and Informatics Engineering, Information System Engineering (SUNY)
- **B.Sc.:** 2020, Binghamton University, Thomas J. Watson College of Engineering and Applied Science, Computer and Information Science

PROFESSIONAL EXPERIENCE AND AWARDS:

- 2019-2020 Teaching Assistant at Binghamton University.
- 2020 Merit-Based Dean's Honor List at Istanbul Technical University.
- 2021-2022 Software Developer at ATEZ Yazılım Teknolojileri A.Ş.

PUBLICATIONS, PRESENTATIONS AND PATENTS ON THE THESIS:

- **Taşkın G.**, Sandıkkaya M. (2023). Comparison of Security Frameworks for SMEs. *ELECO2023 - 14th INTERNATIONAL CONFERENCE on ELECTRICAL and ELECTRONICS ENGINEERING*, November 30 - December 2, 2023, Bursa, Turkey.