Received: 26 September 2024 | Revised: 15 January 2025 | Accepted: 11 February 2025 | Published online: 6 March 2025

Archives of Advanced Engineering Science
2025, Vol. 00(00) 1–19
DOI: 10.47852/bonviewAAES52024438

RESEARCH ARTICLE

Review and Design of Business Domain-Specific Cybersecurity Controls Framework for Micro, Small, and Medium Enterprises (MSMEs)

Shekhar Pawar[1],* and Hemant Palivela[1]

[1]Swiss School of Business and Management Geneva, Switzerland

Abstract: Micro, small, and medium enterprises (MSMEs) play a crucial role in the global economy, contributing significantly to employment opportunities, national income, and GDP. With Industry 4.0, there has been an increase in digitization in MSMEs, which has caused an increased cyberattack surface. Even though there are popular cybersecurity standards and frameworks, adoption of those at a significant level is lagging in MSMEs, causing one out of two such companies to be facing cyber threats. MSMEs have limited resources, less cybersecurity knowledge, and differing priorities for their business. Existing cybersecurity standards and frameworks are generic in nature, not specific to their business domain's security needs. This paper assesses the current cybersecurity posture of MSMEs and the problems they face in implementing cybersecurity and shares insights on the proposed new framework, which is providing business domain-specific least cybersecurity control implementation based on the Confidentiality, Integrity, and Availability (CIA) Triad and Defense in Depth concept.

Keywords: MSME, cybersecurity, cybersecurity framework

1. Introduction

Each country has its own definition of a micro, small, and medium-sized enterprise (MSME). In countries like India or the continent of Africa, these companies are known as MSME [1, 2]. Some nations even refer to these companies as small and medium-sized enterprises (SMEs) or small and medium-sized businesses (SMBs). The term SMB is used in various countries around the world, often interchangeably with SME [3–6]. The primary factors used to categorize businesses or enterprises are their workforce size and/or their annual turnover range [7]. SMEs account for 55% of the GDP in developed nations and support 70% of employment worldwide [8, 9]. Digitization has greatly changed how industries operate in the 21st century, ushering in the industrial revolution. SMEs today must embrace the digital era to meet the demands of a competitive market. This involves a wide range of components, from shop floor to top floor, including IoT devices and cloud computing [10]. While there are advantages, it is also critical to recognize that these organizations now have a larger surface area for cyberattacks. Recent research indicates a reasonable probability of a cyber breach for half of SMEs [11]. Given that over 50% of them are targets of cyberattacks, SMEs are always at high risk from cyber threats [12, 13].

Information security and cybersecurity are distinct fields, with cyberspace defined by Internet connectivity and physical entities, even without the Internet. Cybersecurity focuses on information availability, confidentiality, and integrity, while cyberspace is defined by connectivity between physical entities, clarifying the term "cybersecurity" [14].

Recent data on cyberattacks targeting SMEs underscore the need for research projects to understand the specific issues they face. The authors conducted a comprehensive survey with 115 SMEs worldwide, involving top management executives. The results will be beneficial to readers and the authors' analysis of the findings. The next step is to determine the recommended resolution for SMEs after collecting and processing the inputs. Understanding the issues faced by SMEs with self-defense and their current cybersecurity implementation is crucial.

The authors shall describe how they arrived at the conclusion that SMEs must adopt cybersecurity controls in a manner distinct from the conventional cybersecurity framework or standards, in the sections that follow and their subsections.

2. Related Work

As ISO 27001 provides a formal set of specifications for controls to mitigate information security risks, most enterprises employ it as their principal information security standard or framework. For any qualifying organizations, it also offers formal certification for Information Security Management Systems (ISMS) [15]. ISO 27001:2013 contains 114 controls, which are mapped to 14 distinct objectives [16]. Guidelines for implementing the controls outlined in ISO 27001:2013 are provided by ISO/IEC 27002:2013 [17]. The recently released ISO 27001:2022 contains 93 controls, which are divided into four categories. The 93 controls comprise 34 technological controls, 14

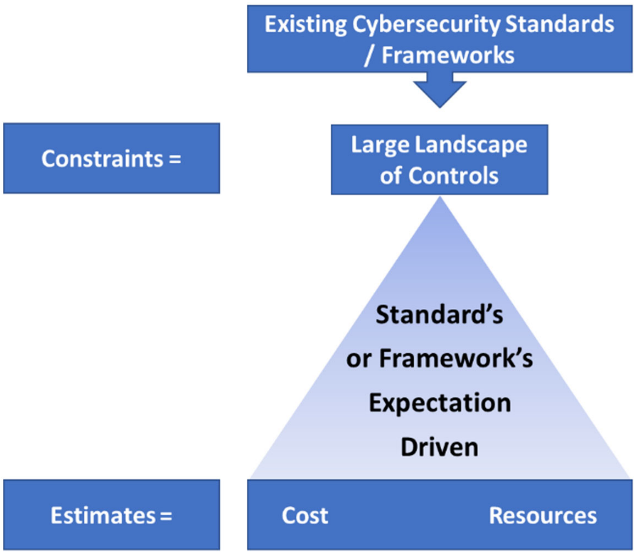
*Corresponding author: Shekhar Pawar, Swiss School of Business and Management Geneva, Switzerland. Emails: shekhar@ssbm.ch; shekharpawarmgm@gmail.com

physical controls, 8 personnel controls, and 37 organizational controls [18–21]. In addition to ISMS, the National Institute for Standards and Technology (NIST) cybersecurity framework, which is based on five key functions – identify, protect, detect, respond, and recover – is also widely accepted. Irrespective of an organization's size, the cybersecurity of its vital infrastructure is the main focus of this framework. The NIST framework is distinctive in that it can be applied globally across all sectors and is not country- or industry-specific. It considers risk management at the organization-wide level for providing essential services and continuously enhances the environments of industrial control systems and information technology (IT) [22]. NIST Special Publication 800-53 Revision 4 provides approximately 900 or more unique security controls from 18 distinct control families, which assist in risk reduction, information protection, the overall cybersecurity framework, and security standards. The most recent framework developed for a risk-based approach is the NIST CSF. It is important to realize that even the NIST CSF is evolving, similar to ISO 27001, and that new cyber threats are emerging every week [23–26]. Assessment and Gap Analysis, Implementation, Training and Awareness, and Ongoing Annual Maintenance are important cost considerations for ISO 27001 and NIST. Depending on the number of employees and other variables, the cost of these certifications, even for SMEs, typically reaches thousands of US dollars for each phase [27, 28].

The Security System Engineering Capability Maturity Model (SSE-CMM) is a framework consisting of two components: System Security Engineering (SSE) and the Capability Maturity Model (CMM). The model consists of eleven process areas and five CMM levels: initial, repeatable, defined, managed, and optimized. The maturity stages are based on the organization's IT governance practices. Initially, organizations may not have prior planning, leading to a reactive IT implementation. At maturity level 2, organizations follow a pattern without a formal approach, achieving repeatable maturity. At maturity level 3, organizations have formal operating procedures, reaching level 4 with multiple indicators for specific goals. At maturity level 5, organizations implement IT governance best practices, achieving optimized maturity [29]. The security goals of IT products or system operating environments are the primary focus of the Common Criteria (CC) framework [14]. In addition to all of these frameworks and standards, enterprises are increasingly adopting the Zero Trust Concept these days. This idea follows the "no trust" policy for any request for internal or external access from a system or user [30].

CC is an excellent tool for assessing the security of IT products, but getting ready for it takes a substantial investment of funds and time. SSE-CMM does not specify particular procedures; instead, it provides guidelines. The development of the information security management systems (ISMS) that businesses need is aided by the ISO/IEC 27001 standard. Many organizations find it challenging to keep up with the latest security knowledge and to develop it for a variety of reasons [16, 31]. The successful implementation of the NIST framework still requires substantial resources, as some areas have not yet been properly mapped out. Smaller organizations see little value in adopting the Framework in an incident where there is little to no risk of occurrence because they remain skeptical about their potential as targets for attacks [23, 32]. One of the NIST framework's drawbacks is that, due to it being based in the USA, the majority of its documentation primarily focuses on US laws and regulations [22, 33, 34]. Nevertheless, this framework is still developing and has few gaps. Zero trust is a commendable idea, but putting it into practice successfully requires substantial resources, and it doesn't even fully address every need in a particular domain [35].

Figure 1
Current paradigm of cybersecurity


Existing Cybersecurity Standards / Frameworks
Constraints =
Large Landscape of Controls
Standard's or Framework's Expectation Driven
Estimates =
Cost
Resources

Studies demonstrate that SMEs globally encounter challenges such as funding shortages, skilled labor shortages, and resource scarcity. Strategic planning, which identifies the business environment and strategic objectives, is pivotal for the growth and sustainability of these organizations. Top management then devises initiatives to achieve these objectives. Owing to their constrained budgets and limited resources, SMEs find it arduous to invest in fields such as cybersecurity as they do not align with their strategic goals [36–39].

Additionally, according to a summary of research findings, the cybersecurity frameworks and standards currently in use suffer from being costly to implement, time-intensive, requiring extensive expertise, and lacking clear or useful guidance throughout the implementation process. One significant finding is that none of the frameworks or standards currently in use are intended for SMEs and do not address their business objectives or concentrate on the essential aspects of their industry. As shown in Figure 1, at the highest level, there is a vast array of controls that must be satisfied to meet the required framework or standard.

3. Methodology

Referring to the preceding sections, it is clear that SMEs, the backbone of the global economy, are increasingly being targeted by cyber threats. Despite established cybersecurity standards, the root cause of these threats remains elusive. Researchers conducted a survey in Q3 2021 among 115 SMEs across key business sectors to understand their current state and cybersecurity challenges. The survey aimed to understand the adoption of cybersecurity standards, the level of implementation of these controls, the types of cyber threats they have faced, and what is preventing SMEs from implementing these controls to safeguard their enterprise and mission-critical assets. The research underscores the critical need for SMEs to address these issues and ensure their ongoing success in the global economy.

The purpose of this study is to gather direct feedback from SMEs in order to understand the current implementation of

Table 1
Interpretation of the mean scale for belief, concern, and practice

SME's domain	Sample size	Actual response
Banking, Financial Services, and Insurance (BFSI)	20	11
E-commerce	20	6
Education	20	3
FMCG	20	4
Hospitality	20	4
Insurance	20	4
IT industry	50	38
Logistics	20	4
Manufacturing	20	8
Media	20	5
Pharmaceutical	20	2
SAAS	20	5
Telecommunication	20	4
Other	60	17
Total	**350**	**115**

cybersecurity controls, observe the difficulties these businesses face, and perform a comprehensive gap analysis of the cybersecurity posture within SMEs and the associated risks. The aim is to create a well-organized set of suggested recommendations that can be used as a fresh framework to address the problems that have been identified.

Key research questions concern whether SMEs have adopted any cybersecurity standards or frameworks, the administrative, logical (or technical), and physical controls they have implemented, how frequently they conduct cybersecurity awareness among employees, the cyber threats they have faced, and the biggest obstacles faced by the organization in this area.

The study hypothesizes that the expectations established by current cybersecurity standards or frameworks are not in accordance with the specific domain requirements of SMEs or the overall benefit for SMEs to invest in or relate to them.

This study employs a quantitative technique and a research survey to address the proposed questions. In the research survey, participants who are SME leaders, mostly C-level executives such as CEO, CTO, CISOs, etc., will be considered. Refer to Appendix A for the detailed questions asked in this research survey.

Table 1 displays the actual response from the participating SMEs as well as the sample size chosen for this study. Only 115 of the 350 top management SMEs approached by the research offered their time to take part in the studies. Top management from SMEs, who are involved in cybersecurity decisions, execution, and other areas, were contacted to obtain accurate input. Many of the directors, owners, business unit heads, C-level executives (CEO, CISO, CTO, etc.,), and others who work in SMEs are regarded as the appropriate and authorized participants to contribute the important information for this study. The SMEs who participated were meticulously selected to gather feedback from diverse business sectors.

SMEs from various countries, including India, the US, Australia, the UAE, Russia, Sweden, South Africa, Indonesia, Norway, Israel, Singapore, Sri Lanka, Bangladesh, Ireland, the UK, Ghana, Cyprus, Kenya, and Nigeria, took part. The authors received a broad range of participation from SMEs across a variety of business domains, including consulting, education technology, executive coaching, healthcare, hospitality, insurance, logistics, supply chain management, human resources, pharmaceuticals, renewable energy, maritime, travel technology, oil industry, online services, exports, financial services, fast-moving consumer goods, Fintech, Banking, Financial Services, and Insurance (BFSI), and more. For further details on the participating companies, please refer to Appendix B.

4. Analysis of Results

In this section, the valuable first-hand information from SMEs is examined and discussed. As shown in Figure 2, the data show that 58% of the participating SMEs were established enough in their industry to last for a number of years, indicating that they must have realized how critical cybersecurity is to their expanding company.

Figure 2
Age of SME who participated in survey

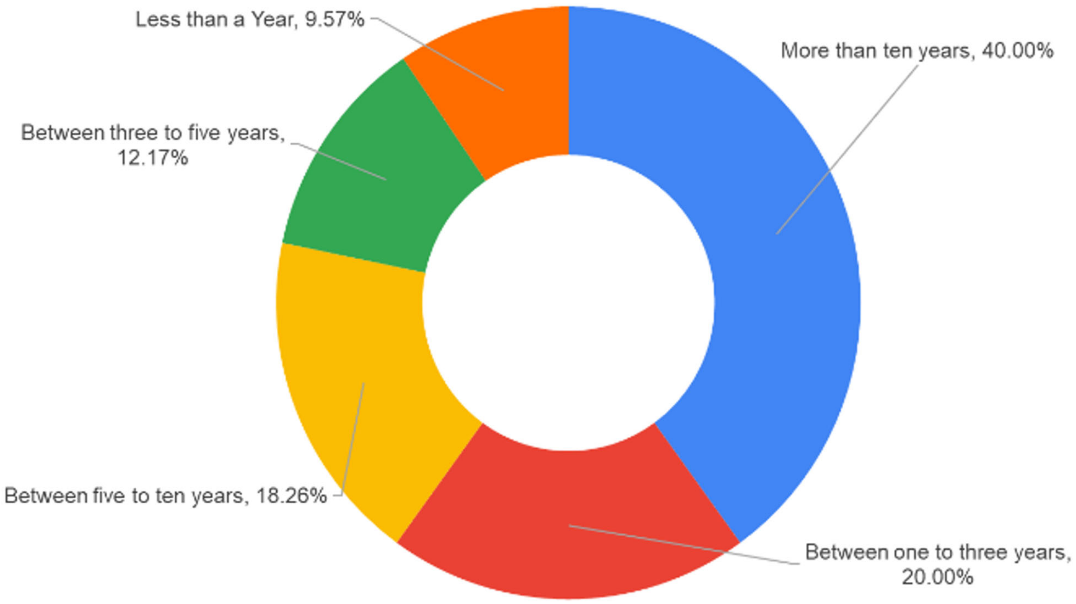
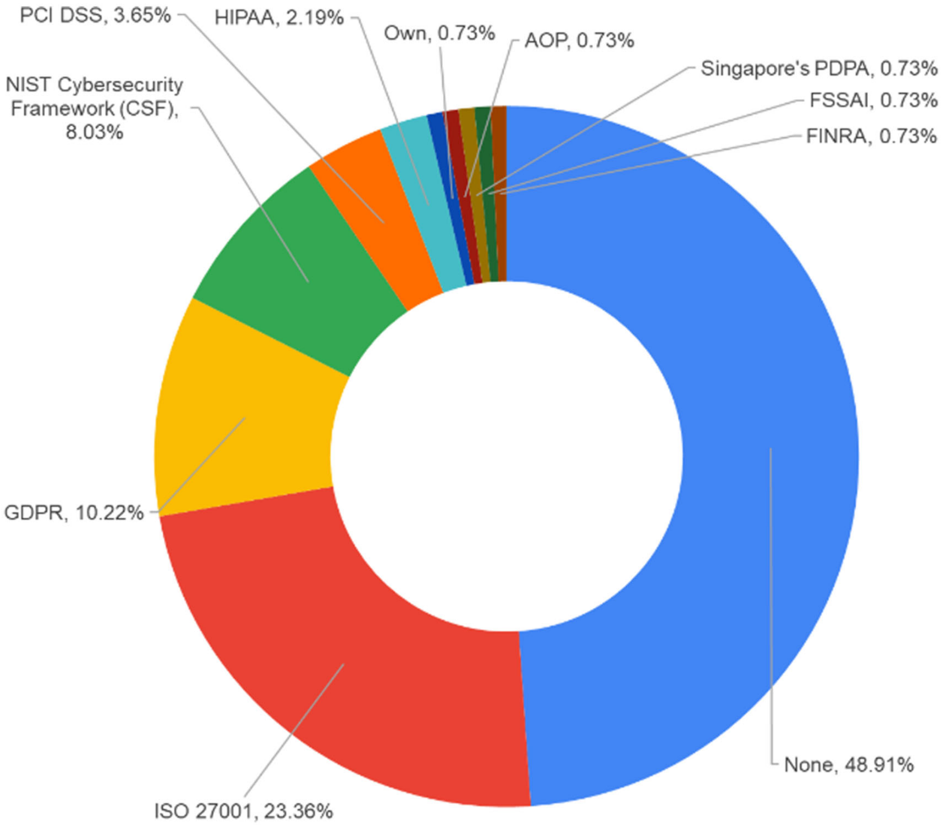


Figure 3
Security standards/frameworks implemented in SMEs



According to the authors' investigation, more than half of SMEs do not currently have any cybersecurity standards or frameworks in place. The insights into the cybersecurity frameworks and standards used by SMEs, and the number of SMEs utilizing them, are as follows: AOP (1), FINRA (1), FSSAI (1), GDPR (14), HIPAA (3), ISO 27001 (32), NIST Cybersecurity Framework (CSF) (11), None (67), Own (1), PCI DSS (5), and Singapore's PDPA (1). As illustrated in Figure 3, approximately 23% of the overall count uses ISO 27001, also known as ISMS, while roughly 23% utilize GDPR. The Health Insurance Portability and Accountability Act, the Payment Card Industry Data Security Standard (PCI DSS), the EU General Data Protection Regulation (GDPR), the Financial Industry Regulatory Authority (FINRA), the Food Safety and Standards Authority of India (FSSAI), and the Singapore Personal Data Protection Act (PDPA) are more specific compliance requirements that any organization can meet, but they are not comprehensive cybersecurity standards or frameworks that can protect all of an SME's critical assets. Fewer than 8% of SMEs have adopted NIST's CSF. It was surprising to learn that approximately 1% of SMEs are also attempting to implement their own standard or framework to have protection against cyber threats, in addition to the few more frameworks or best practices that they have adopted out of compliance requirements or with the intention of improving specific areas related to their cybersecurity posture.

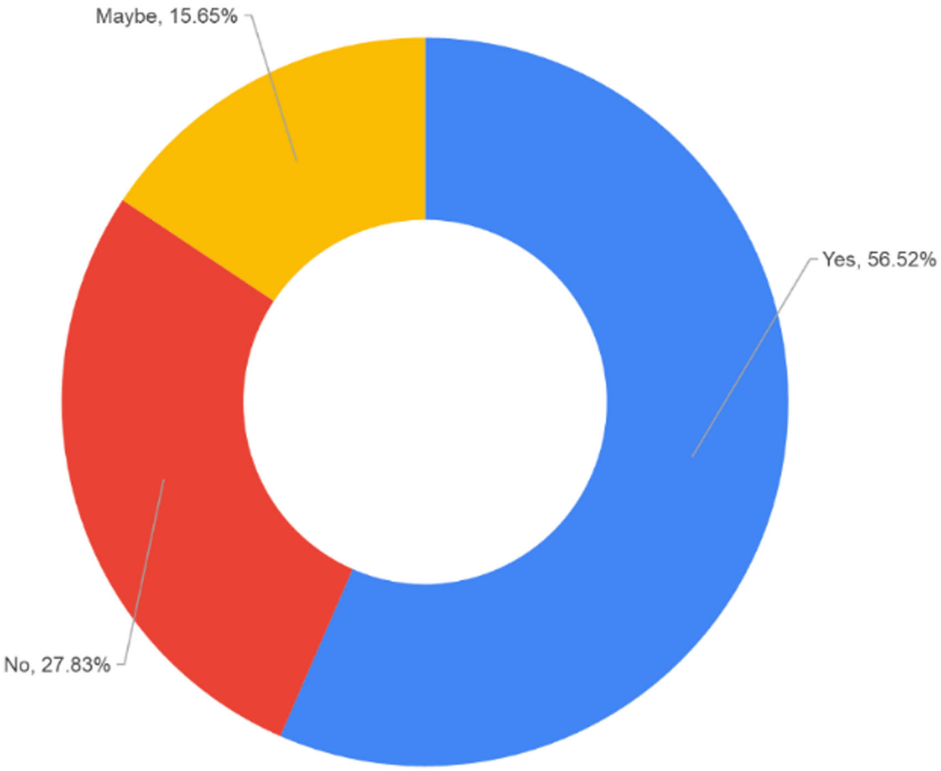
The biggest risk is that half of SMEs are completely exposed to cyber threats. Additionally, a large number of SMEs that are attempting to forgo robust protection at various levels in favor of merely implementing certain controls related to compliance or best practices run the risk of being nearly entirely vulnerable to cyberattacks. Assuming that NIST and ISO 27001 have been correctly implemented within a short period of time, more than two-thirds of SMEs remain severely exposed to cyber threats.

Figure 4 illustrates that approximately 28% of SMEs do not have any cybersecurity controls in place. It indicates that they have "ZERO" or "NO" cybersecurity safeguards in place. Additionally, nearly 16% of SMEs are unsure about the cybersecurity controls they have in place. It's a challenging situation; some may believe they are secure online, while others remain unsure. It also demonstrates top management's lack of awareness regarding cybersecurity implementation in the company to which they are affiliated. Just over half of small and medium-sized enterprises reported having cybersecurity controls in place. This group may have embraced cybersecurity standards such as NIST or ISO 27001, while the remainder may have self-identified random controls providing them assurance of online security.

The three primary categories of security controls in any cybersecurity posture are administrative, logical or technical, and physical controls. Physical controls are visible, observable measures that are accessible to all individuals connected to SMEs. Technical controls refer to the application of technology used to accomplish specific cybersecurity objectives. Administrative controls are primarily concerned with the policies, guidelines, and procedures that all individuals involved in the organization are required to adhere to in order to accomplish cybersecurity objectives. The authors looked for SMEs that implemented these three types of controls.

A large number of physical controls which are put in place to improve cybersecurity posture are monitoring-related, helping in the areas of people, process, and technology. These controls are highly helpful in guarding critical infrastructure or valuable assets

Figure 4
Any security control implementation for SME



from threats of sabotage, theft, or other human- or machine-driven attacks [40]. Few insights into the physical controls and their values as to how many SMEs are using them are as follows: access cards (36), biometric access controls (33), CCTVs (61), environmental controls like HVAC and humidity controls (16), fences (21), fire suppression (34), gates (44), guards (34), motion sensors (9), none (28), security badges (19), security lighting (11), surveillance cameras (30), and virtual (2). Figure 5 illustrates that, of the businesses that report having cybersecurity controls in place, about 8% of SMEs do not have any physical cybersecurity controls in place. The most popular physical cybersecurity controls were access cards (approximately 10%), physical gates (12%), and CCTV (16%). Moreover, it was found that the least used physical controls were motion, environment, and security lighting. It seems that SMEs are not implementing sufficient physical controls.

Technical controls are vital for critical cybersecurity functions to operate properly in any organization. In functional domains like monitoring, logging, encryption, access control, alert mechanism, etc., these controls can carry out their vital role [41]. The following are interesting details of the technical controls and their values regarding how many SMEs are utilizing them: Access Control Lists (ACLs) (29), Antivirus Software (77), Authentication Solutions (43), Constrained Interfaces (12), Encryption Measures (28), Firewalls (61), Intrusion Detection Systems (IDSs) (20), Intrusion Protection Systems (IPSs) (14), and None (25). As depicted in Figure 6, around 8% of SMEs among the businesses that stated they had cybersecurity controls in place do not have any technical controls implemented. According to feedback from SMEs, the most extensively used technical controls are firewalls, which are employed by approximately 20% of all technical controls, and antivirus software, which is used by around 25% of total controls. This trend is a significant indicator of gaps in the implementation of technical controls. This underscores the need for SMEs to implement more robust security measures, such as antivirus software, to safeguard their computers against potential threats and maintain a competitive advantage in digitalization.

Here are intriguing insights into the administrative controls and their values regarding SME utilization: Security Guidelines (48), Security Policies (58), Security Procedures (37), and None (37). As depicted in Figure 7, of the enterprises that reported having cybersecurity controls, over 20% of SMEs lacked any cybersecurity-related policies, guidelines, or procedures. A security policy should offer SMEs comprehensive, lucid approaches, and well-defined best practices, and about one-third of SMEs have one in place. Approximately 80% of SMEs lack any form of procedure to support stakeholders within an organization, and over 73% of SMEs lack security guidelines. SMEs frequently lack policies and procedures for cybersecurity best practices, resulting in potential negative consequences. Enterprises should establish and implement cybersecurity procedures, underpinned by fair policies and guidelines. Regular updates are vital to account for evolving business objectives, external factors, and technological advancements. These controls are essential as they impact the organization’s human factors and should be updated to ensure the protection of all employees [42].

As Figure 8 clearly illustrates, approximately 34% of enterprises have never provided their staff with cybersecurity training. People who work for or are connected to the enterprise organization – such as employees, vendor teams, partners, guests, etc., – are the weakest link that makes successful cyberattacks possible. Enhancing cybersecurity awareness among all of them through regular cybersecurity awareness training is crucial, as the effectiveness of other cybersecurity controls will be compromised

Figure 5
Types of physical security control implementation among SMEs which have those implemented

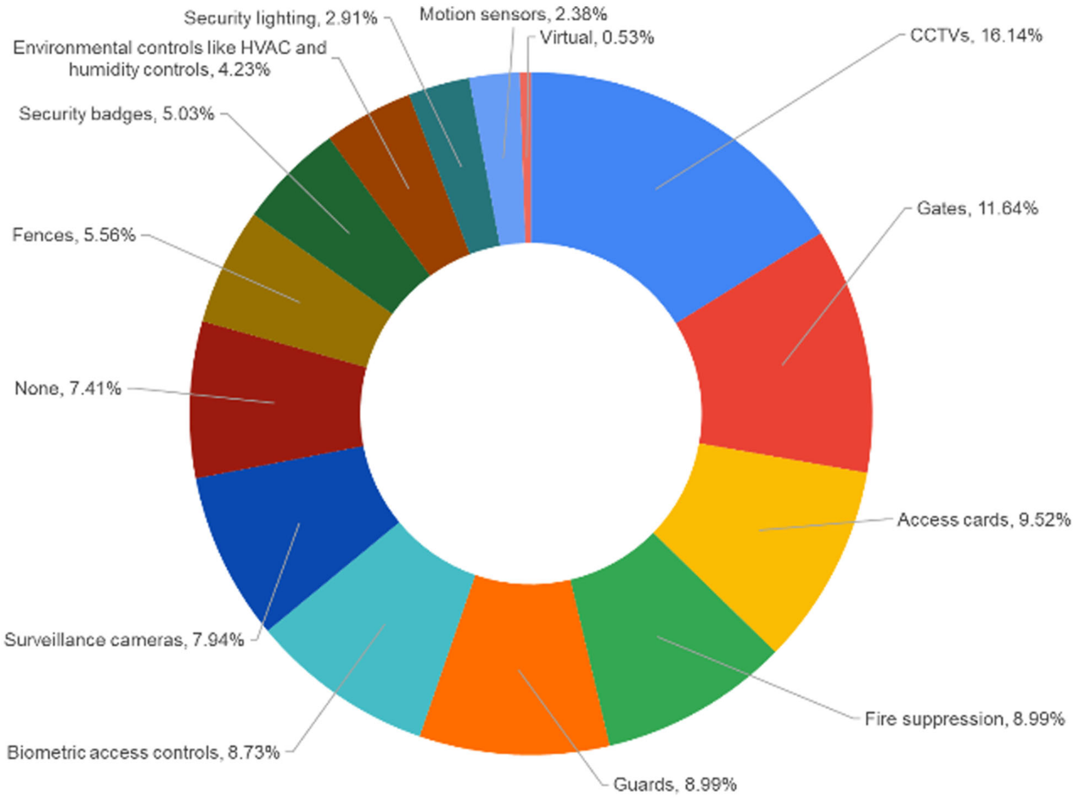


Figure 6
Types of technical security control implementation among SMEs which have those implemented

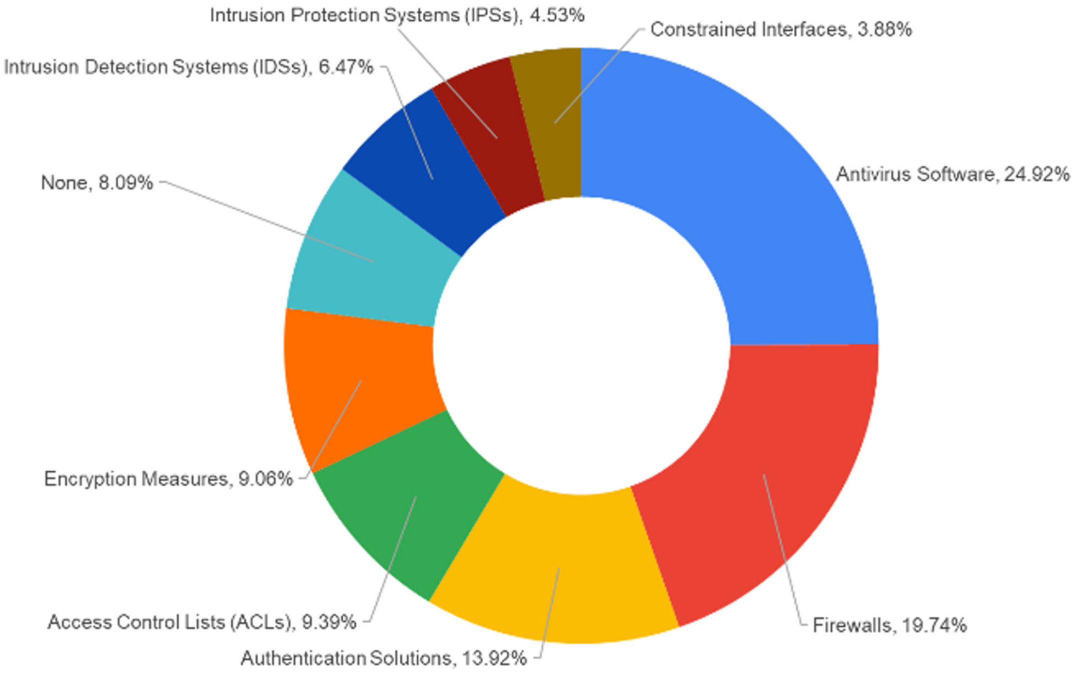


Figure 7
Types of administrative security control implementation among SMEs which have those implemented

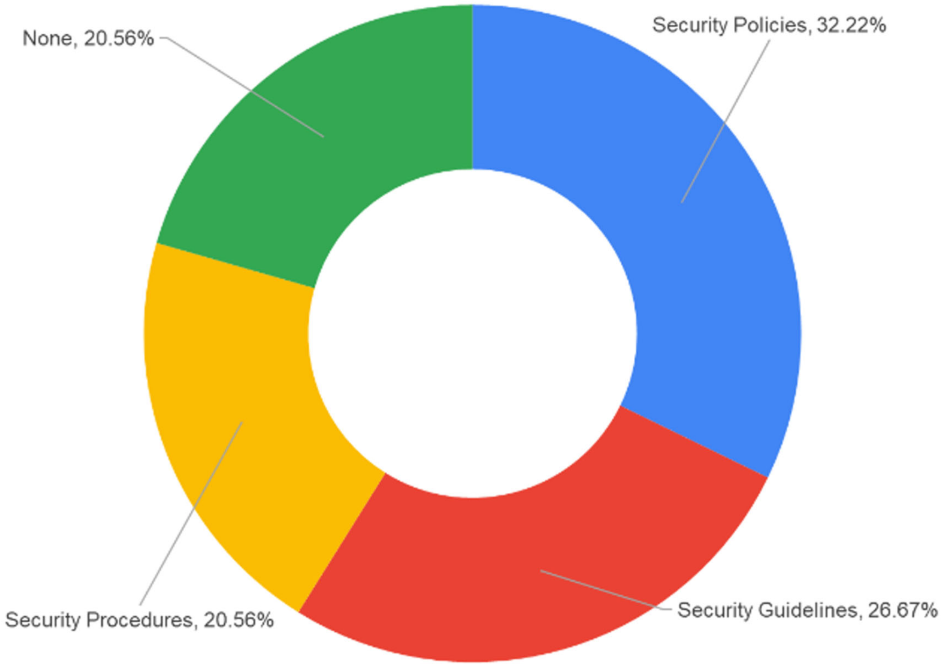
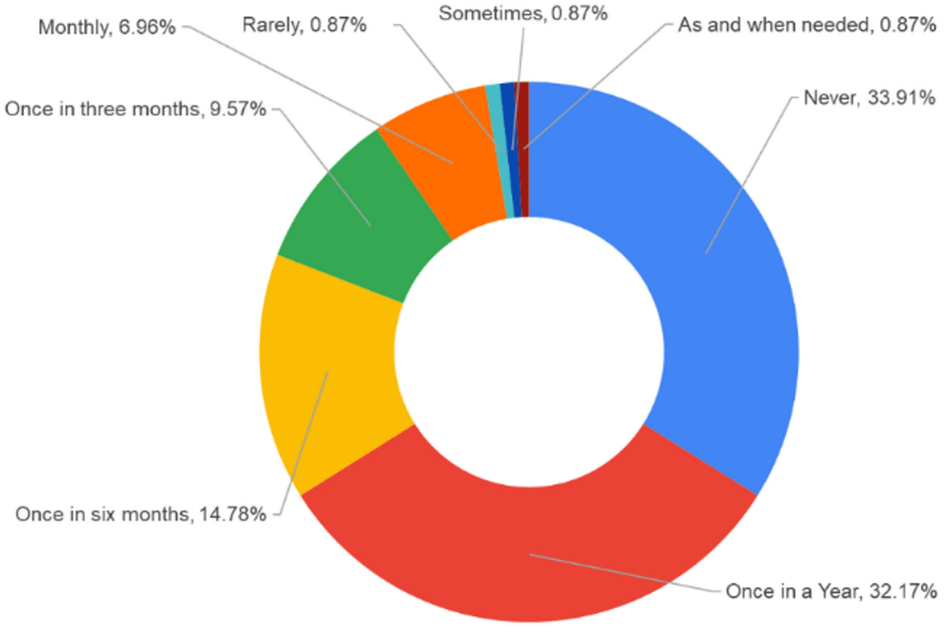


Figure 8
Frequency security awareness training for employees in SME

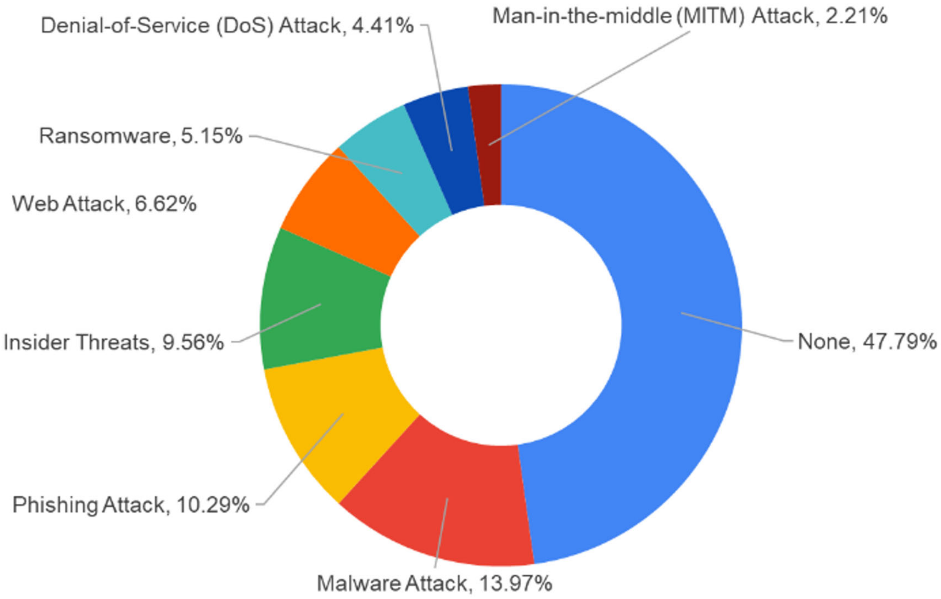


without it. Effective message delivery, in line with the significance of the information, who should be communicating it, avoiding shortcuts to get around processes, commitments, norms, salience, affect, and even ego, are all factors that must be considered when improving cybersecurity training [43].

When authors attempted to establish which cyber threats most SMEs faced, about 48% of SMEs stated they had not yet experienced a cyberattack. Cyber threats that most SMEs have encountered in the past include ransomware, phishing, malware, insider threats, web attacks, Denial-of-Service (DoS) attacks, and Man-in-the-Middle (MITM) attacks.

Examining the insights into the cyber threats faced by SMEs and the values indicating how many SMEs are encountering them: Denial-of-Service (DoS) Attack (6), Insider Threats (13), Malware Attack (19), Man-in-the-Middle (MITM) Attack (3), Phishing Attack (14), Ransomware (7), Web Attack (9), and None (65). As shown in Figure 9, insider threats account for around 10%, phishing attacks for over 10%, and malware attacks for

Figure 9
Cyber threats faced by SMEs



approximately 14% of all cyber threats that SMEs have faced in the past. Malware is a combination of malicious software and intent, as the name suggests. Cybercriminals create these software codes with the intention of attacking targets, which can be any individual's or company's system. These malicious programs use Trojan horses, spam email attachments, and other methods to successfully infiltrate the victim's computer [44]. Insider cyber threats, which are commonly known, are created by the cybercriminal mindset that happens among an enterprise's stakeholders, including employees, vendors, partners, and even visitors [45]. In the digital age, shop floors and top floors are connected to cloud platforms with web applications, and cybercriminals employ various techniques to hack these applications [46]. Ransomware attacks are those in which cybercriminals encrypt the victim's computer and demand a ransom for the decryption key in order to restore the machine to normal functioning. These kinds of attacks aim to steal money or even data [47].

It is possible to mitigate or eliminate these cyber threats to a certain degree by implementing diverse physical, logical, and administrative measures.

Details about the issues faced by SMEs and their values as to how many SMEs are using them are as follows: the cost involved in implementing cybersecurity controls (52), the lack of resources to implement and maintain (38), uncertainty about which cybersecurity controls to implement (42), other business priorities being more important (37), lack of time (1), not finding a roadmap to invest in Cybersecurity control implementation (24), not having thought of it now (1), not facing any problem (1), and the available cybersecurity standards or frameworks needing a significant investment (17). Figure 10 provides the most crucial understanding of SMEs, which will aid in comprehending the fundamental problems preventing SMEs from implementing cybersecurity controls. As is evident, when it comes to implementing cybersecurity looking at all inputs, approximately 25% of SMEs are facing problems with budget allocation or financial investment. Approximately 8% of SMEs believe that adopting current cybersecurity frameworks and standards will require significant financial outlays. Furthermore, around 20% of SMEs are uncertain as to which cybersecurity controls are necessary for them to implement and which are not. Approximately 18% of SMEs believe they lack the resources necessary to establish and/or maintain cybersecurity controls.

SMEs often struggle to justify the ROI associated with strengthening their cybersecurity posture, due to the emphasis placed on the inventory of cybersecurity controls in cybersecurity frameworks and standards. They struggle to connect cybersecurity to business objectives and may be observing how these standards are implemented to fulfill the objective of providing a set of controls for businesses. The lack of a solid justification for cybersecurity as a necessary component for business survival and expansion is a significant issue.

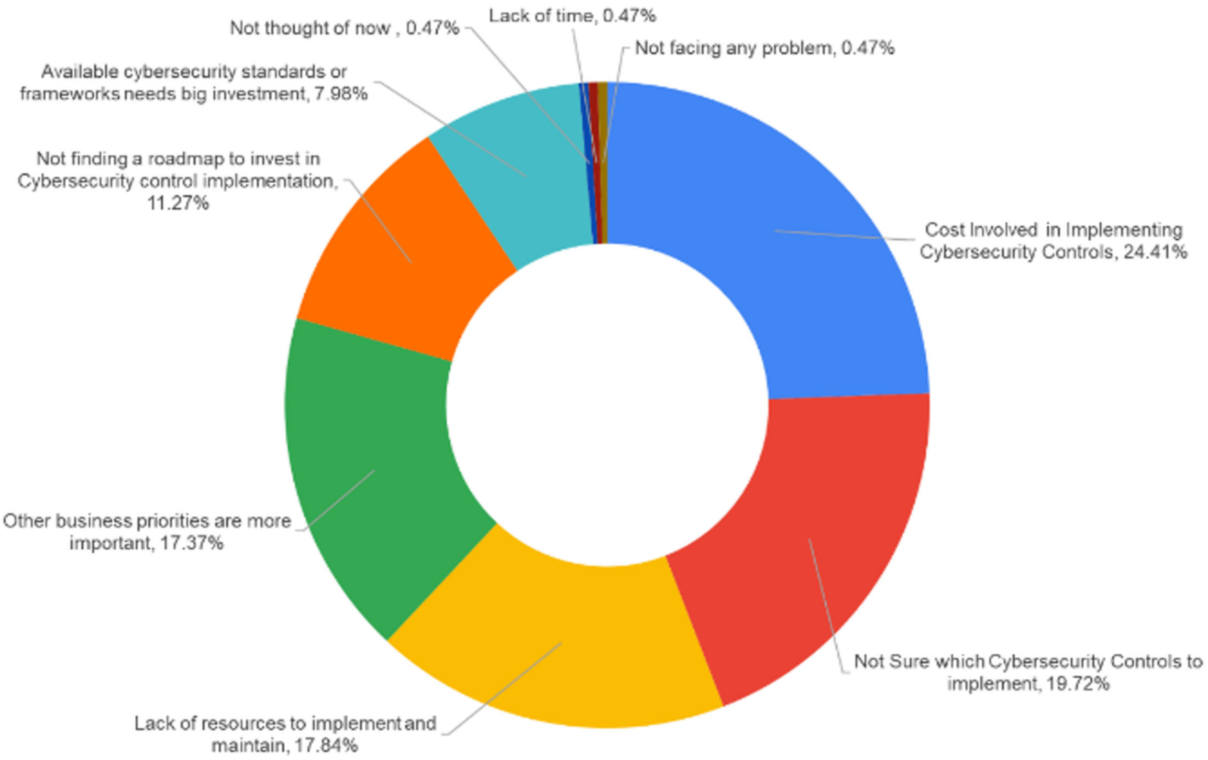
The research suggests that SMEs require access to a cybersecurity framework aligning with their business objectives and providing step-by-step instructions for implementing minimal cybersecurity controls. SMEs are currently lagging in implementing administrative, technical, and physical controls, and there are gaps in cybersecurity awareness training for employees. Only a few SMEs have embraced he available cybersecurity frameworks and standards. Regarding cybersecurity implementation, this study hypothesizes the assumption that the SMEs' current cybersecurity posture is not in a good state because of a number of problems.

5. Core Cybersecurity Concepts Helping Prioritization

The basis of all cybersecurity frameworks and standards for the last few decades have been Defense in Depth (DiD) and Confidentiality, Integrity, and Availability (CIA Triad).

Enterprises can achieve optimal availability by preventing any destruction of their cybersecurity, maintaining confidentiality in their cybersecurity posture by avoiding disclosure, and improving integrity in cyberspace by preventing unauthorized entities from altering or modifying their work [48]. While each of these three areas is distinct and has a different goal, there is always some overlap between them, as seen in Figure 11 of the CIA Triad Venn diagram.

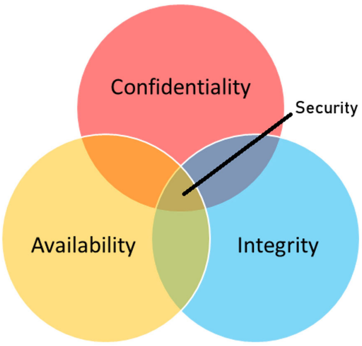
Figure 10
List of issues faced by SMEs while forming cybersecurity posture



Cybersecurity controls, which can be administrative, logical, or physical, are impacted by an organization's people, processes, and technology. Every business domain has distinct critical assets necessary for survival and growth, and each asset has distinct priorities extending to the CIA triad areas.

In Table 2, an example of an SME's Business-Critical Asset (BCA) is presented, which is further mapped using the CIA triad. Regarding SMEs in the Banking, Financial Services, and Insurance (BSFI) industry, the privacy of financial transactions conducted via their online portal is of utmost importance. It is better to endure a few hours of unavailability for this web portal than to compromise transaction confidentiality. Because of this, BSFI prioritizes confidentiality for this web portal as a crucial asset, with integrity and availability being secondary considerations [49].

Figure 11
CIA Triad

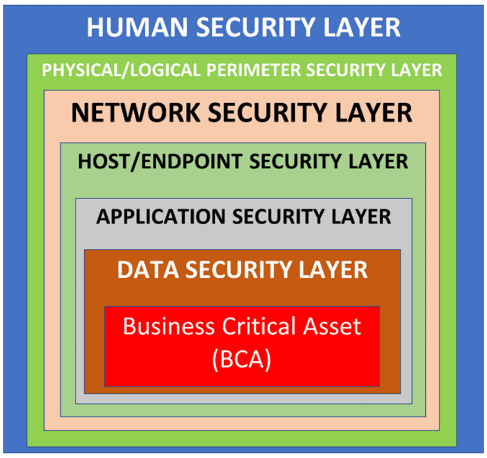


If an SME's primary business is e-commerce, its e-commerce website serves as a crucial business asset. With availability being the most important factor, followed by integrity and confidentiality, the biggest risk is if the website is unavailable for hours or days [50, 51]. An essential asset for the pharmaceutical, drug manufacturing SME will be the system crucial to the drug formula. Merely altering the ingredient composition will result in dangerous products, such as pills or medications. The person consuming it may have been in danger of their life. Integrity is the asset's top priority, meaning no unauthorized events or entities

Table 2
Prioritization in CIA Triad for specific BCA of particular domain

The domain of SME business	SME's business-critical asset (BCA)	Prioritization in CIA triad in ascending order of highest to lowest
Banking, Financial Services, and Insurance (BSFI)	Web Portal for Financial Transaction	Confidentiality, followed by Integrity, And Availability
E-commerce	Online Shopping Web Portal	Availability, followed by Integrity, and Confidentiality
Pharmaceutical Medicine Manufacturing	Drug Formula Software System	Integrity, followed by Availability, and Confidentiality

Figure 12
Defense in depth (DiD) layered concept


HUMAN SECURITY LAYER
PHYSICAL/LOGICAL PERIMETER SECURITY LAYER
NETWORK SECURITY LAYER
HOST/ENDPOINT SECURITY LAYER
APPLICATION SECURITY LAYER
DATA SECURITY LAYER
Business Critical Asset (BCA)

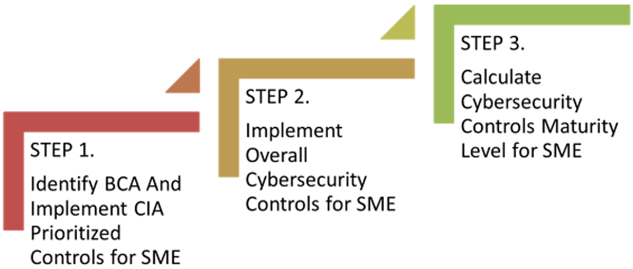
should be able to change the correct formula. After integrity, availability and confidentiality are taken into account [52].

SME top management's opinions are crucial in determining the BCA and CIA triad's importance. They are more knowledgeable about their company's top priorities and can relate to unclear aspects of SMEs. For instance, if an SME operates an e-commerce business listed on a stock exchange, they may prioritize implementing cybersecurity controls based on confidentiality and integrity, or all three CIA triad areas. This is because SMEs risk losing their reputation and potentially facing lawsuits if they violate confidentiality or integrity due to information security breaches.

The Defense in Depth (DiD) model, also known as the "Castle" model, is a widely used cybersecurity innovation developed by the US National Security Agency to enhance security by implementing multiple layers. The BCA is located at the innermost layer of the DiD, as depicted in Figure 12. Each layer's controls will provide protection for the BCA. Data, application, host or endpoint, network, logical or physical perimeter, and human layers are its conceptual layers, which go from the innermost layer to the outermost layer. All these layers are governed by the management of the organization. Businesses should use the mission-centric approach when implementing DiD, which entails protecting BCA from each layer's objectives while also protecting oneself [53].

The human layer, which controls all other controls in the enterprise, is still not thought to be the weakest point for carrying out successful cyberattacks, as was covered in a previous section.

Figure 13
Three stages of recommended solution


STEP 1.
Identify BCA And Implement CIA Prioritized Controls for SME
STEP 2.
Implement Overall Cybersecurity Controls for SME
STEP 3.
Calculate Cybersecurity Controls Maturity Level for SME

6. Three Stages of Recommended Solution

As shown in Figure 13, the authors propose a three-phase solution for SMEs, based on research findings, literature review, and fundamental cybersecurity concepts.

The first step involves identifying BCA and determining top management's CIA triad priorities. SMEs must implement controls to safeguard BCA, affecting their business goals.

The second stage prioritizes implementing the fewest cybersecurity controls across all organizational layers.

The third stage determines the maturity level of the SME's cybersecurity implementation based on the preceding two stages.

The governance, risk management, and compliance framework must be followed by all controls that are implemented in accordance with the framework that is suggested [25, 54–60]. Furthermore, every cybersecurity measure must prioritize human safety above all else [61, 62].

6.1. BCA and CIA-prioritized control implementation

As illustrated in Figure 14, SMEs must examine the asset list and BCA. The BCA is subject to constant change based on a variety of factors, including the business domain of the SMEs, top management's business goals, and several external parameters. An SME may have more than one BCA, but the top management must choose which BCA, if any, to have CIA-prioritized controls for.

Although the authors of this suggested solution to provide stepwise control implementation have shared the prioritized approach of the CIA triad and related cybersecurity controls, even top management is free to choose which areas of the CIA triad to be considered in a one-time implementation.

Different domains may have different business domain critical assets, as Table 3 illustrates. Financial transactions are important to some SMEs, while production or a 24 × 7 presence may be significant to others, and so forth. It is also critical to realize that two distinct SMEs operating in the same domain may have different BCAs and, consequently, differing cybersecurity implementation requirements. The protection from cyber threats can vary depending on whether only one, two, or three elements of the CIA triad for BCA are taken into account. It will possess the highest level of cybersecurity if the CIA trinity is applied to BCA.

6.2. Implement overall cybersecurity controls for enterprise

Any cybersecurity framework is incomplete without taking DiD into account, as stated in earlier sections. This raises the barriers against advanced cyber attacks.

The authors recommend that SMEs enhance the security of the host or endpoint layer, the perimeter layer constructed in both physical and digital bases, and the human layer, as detailed in Table 4 regarding the analysis of research results and literature review. Additionally, SMEs should not overlook networks, applications, or data layers that are publicly accessible beyond the actual boundaries of the business due to the increased exposure factors. DiD implementation at this level will be regarded as level 1. The enterprise will be categorized as Level 2 in DiD implementation according to the authors' recommendation to implement internal network and application layer security. To achieve Level 3, SMEs must additionally incorporate data layer security.

Figure 14
Stage 1: Identify BCA and implement CIA-prioritized controls for SME

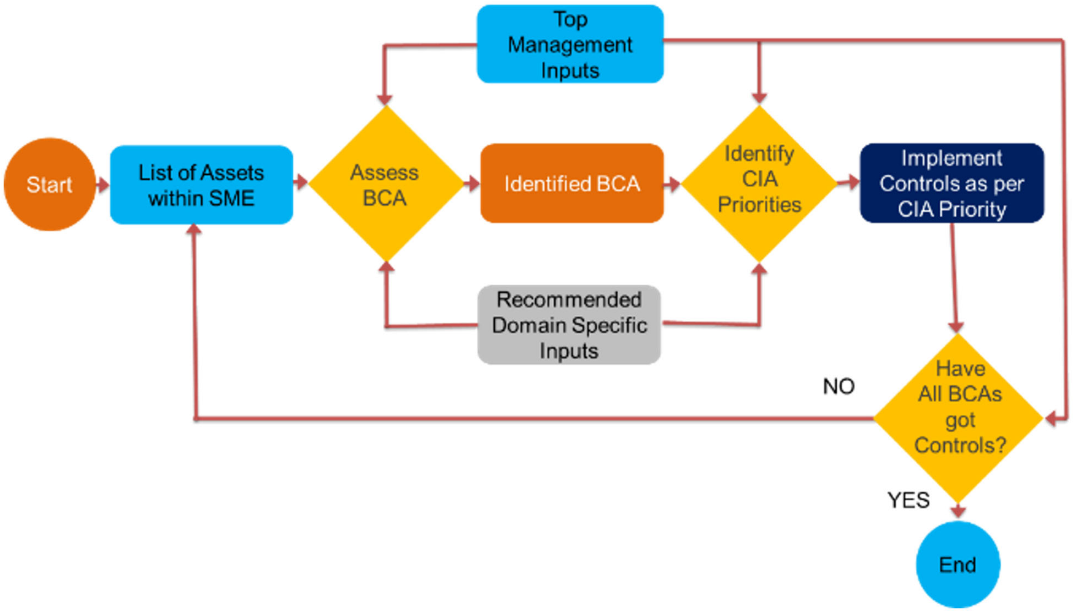

Start
List of Assets within SME
Top Management Inputs
Assess BCA
Identified BCA
Identify CIA Priorities
Implement Controls as per CIA Priority
Recommended Domain Specific Inputs
NO
Have All BCAs got Controls?
YES
End

Table 3
Calculating CIA implementation level for a particular SME

Implementation of cybersecurity controls for BCA with prioritization in CIA triad	CIA triad implementation level
Either Confidentiality, Availability, or Integrity	1 – Low
Either Integrity and Availability, Confidentiality and Integrity, or Confidentiality and Availability	2 – Medium
All Integrity, Confidentiality, and Availability	3 – High

Table 4
Calculating DiD implementation level for a particular SME

Implementation of overall cybersecurity controls considering different layers of DiD	DiD implementation level
Human Layer Security + Physical & Digital Perimeter Security + Host/Endpoint Security + Public Facing Data Layer Security + Public Facing Application Layer Security + Public Facing Network Security	1 – Low
All in Level 1 + Internal Network Layer Security + Internal Application Layer Security	2 – Medium
All in Level 2 + Internal Data Layer Security	3 – High

The authors also recommend that top management consider any layer as a starting point and apply controls effectively to safeguard it. Figure 15 demonstrates how SMEs must implement defense for every layer.

6.3. Calculate SME’s cybersecurity controls maturity level

As previously mentioned in the first two stages, small and medium-sized enterprises (SMEs) have the capability to gradually incorporate cybersecurity controls to protect their primary BCAs and to minimize cybersecurity risks at every level of the organization. The authors’ recommended actions empower top management to select the controls to implement in order to meet organizational objectives or safeguard the company’s vital areas.

Top management of any SME understands their business better. They are better positioned to assess the effects of any changes made to any parameter related to their corporate goals.

One of the key ingredients in the implementation of cybersecurity controls should be top management’s consideration of business priorities. It provides a paradigm shift in the process of enhancing SMEs’ cybersecurity posture, as illustrated in Figure 16. The domain-specific security posture that this new framework offers aids in safeguarding the organization’s most valuable assets.

Cybersecurity frameworks and standards are designed to protect organizations, but SMEs often struggle to implement them due to inapplicable controls. Many SMEs are unaware of potential cyberattacks and require encouragement and support. Top management should recognize the connection between cybersecurity investments and protecting business objectives from cyber threats.

The implementation of BCA-focused cybersecurity controls in conjunction with DiD-focused cybersecurity controls can determine the maturity level of any SME’s cybersecurity posture, as detailed in Table 5. SME will be regarded as having the fewest cybersecurity safeguards in place when they successfully complete both areas to cover every aspect listed. Any such organization would be much

Figure 15
Stage 2: Implement DiD prioritized controls for SME

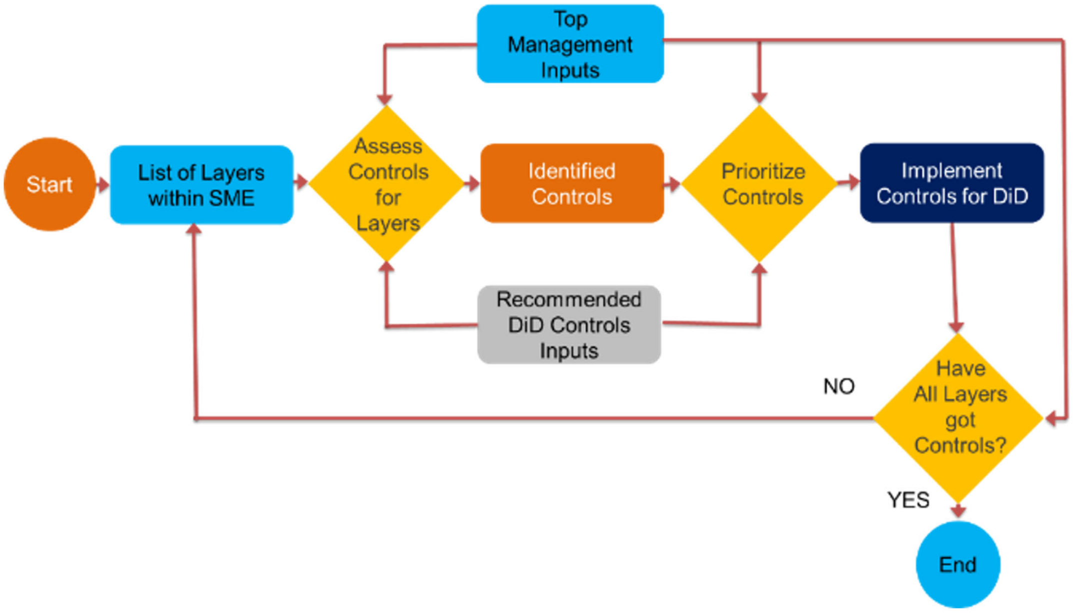

Top Management Inputs
Start
List of Layers within SME
Assess Controls for Layers
Identified Controls
Prioritize Controls
Implement Controls for DiD
Recommended DiD Controls Inputs
NO
Have All Layers got Controls?
YES
End

Figure 16
Paradigm shift in new framework

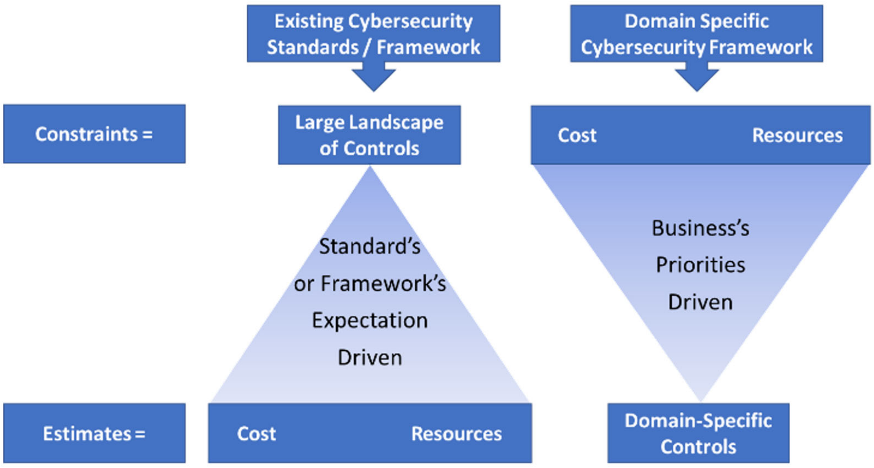

Existing Cybersecurity Standards / Framework
Domain Specific Cybersecurity Framework
Constraints =
Large Landscape of Controls
Cost
Resources
Standard's or Framework's Expectation Driven
Business's Priorities Driven
Estimates =
Cost
Resources
Domain-Specific Controls

Table 5
Calculating cybersecurity maturity level for particular SME

CIA implementation level for particular SME	Implementation of DiD prioritized controls for SME	SME's maturity level
Either Confidentiality, Availability, or Integrity	Human Layer Security + Physical & Digital Perimeter Security + Host/Endpoint Security + Public Facing Data Layer Security + Public Facing Application Layer Security + Public Facing Network Security	1 – Low
Either Integrity and Availability, Confidentiality and Integrity, or Confidentiality and Availability	All in Level 1 + Internal Network Layer Security + Internal Application Layer Security	2 – Medium
All Integrity, Confidentiality, and Availability	All in Level 2 + Internal Data Layer Security	3 – High

more successful with it than with “NO” or “RANDOM” cybersecurity controls.

7. Conclusion and Future Work

It is evident that a large number of SMEs are not prioritizing cybersecurity investments and are already experiencing a variety of issues. Decision-makers within an organization will see benefits that are in line with their business goals if cybersecurity controls are implemented gradually, causing a more attractive framework for them.

To resume, some key points can be listed as follows:

1) SMEs have numerous obstacles to overcome when thinking about putting cybersecurity controls in place. Additionally, it is necessary to assist them in realizing the significance of enhanced cybersecurity posture for the survival and expansion of their business.
2) Due to a paradigm shift, the suggested new cybersecurity framework will address numerous significant problems for SMEs and appeal more to the higher levels of business management.

With some refinements, this framework may eventually be able to assist organizations other than SMEs.

Ethical Statement

This study does not contain any research involving human or animal subjects conducted by the authors.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

Data Availability Statement

Data available from the corresponding author upon reasonable request.

Author Contribution Statement

Shekhar Pawar: Conceptualization, Methodology, Software, Validation, Formal analysis, investigation, resources, Data curation, Writing – original draft, Writing – review & editing, Visualization, Project administration. **Hemant Palivela:** Supervision.

References

[1] Wube, M. C., & Atwal, H. (2024). Supply chain management of micro, small, and medium enterprises (MSMEs) in Africa: A bibliometric analysis. *Journal of Innovation and Entrepreneurship*, *13*(1), 39.

[2] Ahamed, G. T., & Raju, S. A. A. (2023). A review of challenges and opportunities for MSMEs in India: A roadmap for success. *International Journal of Advanced Research in Commerce, Management & Social Science*, *89*, 89–98.

[3] Ullah, A., & Khan, S. D. (2024). Impact of sound decision-making on small and medium businesses in Pakistan. *International Journal of Asian Business and Management*, *3*(2), 177–192.

[4] Guzek, J., & Whillans, A. (2025). Overcoming barriers to employee ownership: Insights from small and medium-sized businesses. *Compensation & Benefits Review*, *57*(1), 64–81.

[5] Okafor, J. N., Anyaegbunam, C. E., & Nwokike, C. E. (2023). The Nexus between family enterprises and the sustainable growth of small and medium-sized businesses in Nigeria: A critical review. *International Journal of Research*, *10*(9), 137–146.

[6] Antonescu, D., & Florescu, I. C. (2024). The small business sector (SMB) and the National Recovery and Resilience Plan in Romania and the European Union. *Revista Romana de Economie*, *59*, 111–113.

[7] Pawar, S. A., & Palivela, H. (2023). Importance of least cybersecurity controls for small and medium enterprises (SMEs) for better global digitalised economy. *Contemporary Studies in Economic and Financial Analysis*, *110B* (978-1-83753-417-3), 21–53. ideas.repec.org/h/eme/csefzz/s1569-37592023000110b002.html

[8] Kahveci, E., Avunduk, Z. B., Daim, T., & Zaim, S. (2024). The role of flexibility, digitalisation, and crisis response strategy for SMEs: Case of COVID-19. *Journal of Small Business Management*, 1–38.

[9] Mhlongo, T., van der Poll, J. A., & Sethibe, T. (2023). A control framework for a secure internet of things within small-, medium-, and micro-sized enterprises in a developing economy. *Computers*, *12*(7), 127.

[10] Müller, J. M., Buliga, O., & Voigt, K. I. (2018). Fortune favors the prepared: How SMEs approach business model innovations in Industry 4.0. *Technological Forecasting and Social Change*, *132*, 2–17. https://doi.org/10.1016/j.techfore.2017.12.019

[11] Tetteh, A. K. (2024). Cybersecurity needs for SMEs. *Issues in Information Systems*, *25*(1), 239–242.

[12] Arroyabe, M. F., Arranz, C. F., de Arroyabe, J. C. F., & Fernandez, I. (2024). Digitalization and cybersecurity in SMEs: A bibliometric analysis. *Procedia Computer Science*, *237*, 80–87.

[13] Hamidi, S., & Gaard, A. (2023). *Information security assessment of the Norwegian SMB-sector: A study of culture, leadership and cost*. Master’s Thesis, UIS.

[14] Bialas, A. (2011). Common criteria related security design patterns for intelligent sensors—Knowledge engineering-based implementation. *Sensors*, *11*(8), 8085–8114. https://doi.org/10.3390/s110808085

[15] Mohamed, N., & Kaur a/p Gian Singh, J. (2012). A conceptual framework for information technology governance effectiveness in private organizations. *Information Management & Computer Security*, *20*(2), 88–106. https://doi.org/10.1108/09685221211235616

[16] Shojaie, B., Federrath, H., & Saberi, I. (2014). Evaluating the effectiveness of ISO 27001: 2013 based on Annex A. In *2014 Ninth International Conference on Availability, Reliability and Security*, 259–264.

[17] Sukmaji, M., Yasirandi, R., & Al Makky, M. (2021). Information security policy and SOP as the access control document of PT. Jui Shin Indonesia using ISO/IEC 27002:2013. *Pilar Nusa Mandiri: Journal of Computing and Information System*, *17*(2), 115–112. ejournal.nusamandiri.ac.id/index.php/pilar/article/view/2282/865, https://doi.org/10.33480/pilar.v17i2.2282

[18] Scarfone, K., Souppaya, M., & Fagan, M. (2024). Mapping relationships between documentary standards, regulations, frameworks, and guidelines. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8477

[19] Surya, I. C., Mulyana, R., & Nugraha, R. A. (2024). BPRDCo SME digital transformation by designing information security using ISO 27001: 2022. *Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi)*, *8*(4), 1242–1253.

[20] McIntosh, T. R., Susnjak, T., Liu, T., Watters, P., Xu, D., Liu, D., . . . , & Halgamuge, M. N. (2024). From COBIT to ISO 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercialising large language models. *Computers & Security*, *144*, 103964.

[21] Chavez, S., Anahue, J., & Ticona, W. (2024). Implementation of an ISMS based on ISO/IEC 27001:2022 to improve information security in the internet services sector. In *2024 14th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, 184–189. https://doi.org/10.1109/Confluence60223.2024.10463392

[22] Dimakopoulou, A., & Rantos, K. (2024). Comprehensive analysis of maritime cybersecurity landscape based on the NIST CSF v2. 0. *Journal of Marine Science and Engineering*, *12*(6), 919.

[23] Toussaint, M., Krima, S., & Panetto, H. (2024). Industry 4.0 data security: A cybersecurity frameworks review. *Journal of Industrial Information Integration*, *39*, 100604.

[24] Islam, M. T., Mission, M. R., Refat, T. K., & Kynatun, M. (2025). Cybersecurity risk assessment frameworks for engineering databases: A systematic literature review. *Strategic Data Management and Innovation*, *2*(01), 224–243.

[25] Wang, W., Sadjadi, S. M., & Rishe, N. (2024). A survey of major cybersecurity compliance frameworks. In *2024 IEEE 10th Conference on Big Data Security on Cloud (Big Data Security)*, 23–34.

[26] Parmar, M., & Miles, A. (2024). Cyber security frameworks (CSFs): An assessment between the NIST CSF v. 2.0 and EU standards. In *2024 Security for Space Systems (3S)*, 1–7.

[27] Leszczyna, R. (2024). ISO/IEC 27001-based estimation of cybersecurity costs with Caspea. In B. Marcinkowski, A. Przybylek, A. Jarzębowicz, N. Iivari, E. Insfran, M. Lang, H. Linger, & C. Schneider (Eds.), *Harnessing opportunities: Reshaping ISD in the post-COVID-19 and generative AI era (ISD2024 proceedings)*. Poland: University of Gdańsk. ISBN: 978-83-972632-0-8.

[28] El-Hajj, M., & Mirza, Z. A. (2024). Protecting small and medium enterprises: A specialized cybersecurity risk assessment framework and tool. *Electronics*, *13*(*19*), 6–12. https://doi.org/10.3390/electronics13193910

[29] Kurniawan, E., & Riadi, I. (2018). Security level analysis of academic information systems based on standard ISO 27002: 2013 USING SSE-CMM. *International Journal of Computer Science and Information Security*, *16*(1), 139–147. www.researchgate.net/profile/Imam-Riadi-2/publication/323029044_Security_level_analysis_of_academic_information_systems_based_on_standard_ISO_270022003_using_SSE-CMM/links/5a7d699c458515dea40f96f0/Security-level-analysis-of-academic-information-systems-based-on-standard-ISO-270022003-using-SSE-CMM.pdf

[30] Muhammad, T., Munir, M. T., Munir, M. Z., & Zafar, M. W. (2022). Integrative cybersecurity: Merging zero trust, layered defense, and global standards for a resilient digital future. *International Journal of Computer Science and Technology*, *6*(4), 99–135.

[31] Alqatawna, J. F. (2014). The challenge of implementing information security standards in small and medium e-business enterprises. *Journal of Software Engineering and Applications*, *07*(10), 883–890. www.scirp.org/html/7-9301952_49991.htm, 10.4236/jsea.2014.710079

[32] Chauhan, M., & Shiaeles, S. (2023). An analysis of cloud security frameworks, problems and proposed solutions. *Network*, *3*(3), 422–450.

[33] Irawan, H., Muhammad, A. H., & Nasiri, A. (2024). Design of cybersecurity maturity assessment framework using NIST CSF v1.1 and CIS controls v8. *Jurnal Inovtek Polbeng Seri Informatika*, *9*(1), 127–136.

[34] Melaku, H. M. (2023). Context-based and adaptive cybersecurity risk management framework. *Risks*, *11*(6), 101.

[35] Alsinawi, B. (2018). *Is the NIST cybersecurity framework enough to protect your organization?* Retrieved from: www.isaca.org, www.isaca.org/resources/news-and-trends/isaca-now-blog/2018/is-the-nist-cybersecurity-framework-enough-to-protect-your-organization

[36] Gamage, S. N., Ekanayake, E. M. S., Abeyrathne, G. A. K. N. J., Prasanna, R. P. I. R., Jayasundara, J. M. S. B., & Rajapakshe, P. S. K. (2020). A review of global challenges and survival strategies of small and medium enterprises (SMEs). *Economies*, *8*(4), 79.

[37] Moeuf, A., Pellerin, R., Lamouri, S., Tamayo-Giraldo, S., & Barbaray, R. (2017). The industrial management of SMEs in the era of Industry 4.0. *International Journal of Production Research*, *56*(3), 1118–1136. www.researchgate.net/profile/Robert-Pellerin/publication/319612802_The_industrial_management_of_SMEs_in_the_era_of_Industry_40/links/5c34e1ec92851c22a364b770/The-industrial-management-of-SMEs-in-the-era-of-Industry-40.pdf

[38] Zutshi, A., Mendy, J., Sharma, G. D., Thomas, A., & Sarker, T. (2021). From challenges to creativity: Enhancing SMEs' resilience in the context of COVID-19. *Sustainability*, *13*(12), 6542.

[39] Prasanna, R. P. I. R., Jayasundara, J. M. S. B., Naradda Gamage, S. K., Ekanayake, E. M. S., Rajapakshe, P. S. K., & Abeyrathne, G. A. K. N. J. (2019). Sustainability of SMEs in the competition: A systemic review on technological challenges and SME performance. *Journal of Open Innovation: Technology, Market, and Complexity*, *5*(4), 100. https://doi.org/10.3390/joitmc5040100

[40] Xie, J., Stefanov, A., & Liu, C. C. (2016). Physical and cyber security in a smart grid environment. *Wiley Interdisciplinary Reviews: Energy and Environment*, *5*(5), 519–542. wires.onlinelibrary.wiley.com/doi/am-pdf/10.1002/wene.202, https://doi.org/10.1002/wene.202

[41] Song, J. G., Lee, J. W., Park, G. Y., Kwon, K. C., Lee, D. Y., & Lee, C. K. (2013). An analysis of technical security control requirements for digital I & C systems in nuclear power plants. *Nuclear Engineering and Technology*, *45*(5), 637–652. www.sciencedirect.com/sdfe/reader/pii/S1738573315300498/pdf, https://doi.org/10.5516/net.04.2012.091

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

[43] Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness Campaigns: Why do they fail to change behaviour?. In *International Conference on Cyber Security for Sustainable Society*.

[44] Abusitta, A., Li, M. Q., & Fung, B. C. (2021). Malware classification and composition analysis: A survey of recent developments. *Journal of Information Security and Applications*, *59*, 102828.

[45] Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. K. R., & Burnap, P. (2020). Impact and key challenges of insider threats on organisations and critical businesses. *Electronics*, *9*(9), 1460.

[46] Luo, C., Tan, Z., Min, G., Gan, J., Shi, W., & Tian, Z. (2021). A novel web attack detection system for internet of things via ensemble classification. *IEEE Transactions on Industrial Informatics*, *17*(8), 5810–5818. www.csit.carleton.ca/wshi/wp-content/uploads/2021/03/09261992-1.pdf, https://doi.org/10.1109/tii.2020.3038761

[47] Madani, H., Ouerdi, N., Boumesaoud, A., & Azizi, A. (2022). Classification of ransomware using different types of neural networks. *Scientific Reports*, *12*(1), 4770.

[48] Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, *10*(3), 21–45.

[49] Al-Alawi, A. I., & Al-Bassam, M. S. A. (2020). The significance of cybersecurity system in helping managing risk in banking and financial sector. *Journal of Xidian University, 14*, 1523–1536. www.researchgate.net/profile/Adel-Al-Alawi/publication/337086201_The_Significance_of_Cybersecurity_System_in_Helping_Managing_Risk_in_Banking_and_Financial_Sector/links/5f288580299bf134049ebe88/The-Significance-of-Cybersecurity-System-in-Helping-Managing-Risk-in-Banking-and-Financial-Sector.pdf

[50] Sutton, S., Khazanchi, D., Hampton, C., & Arnold, V. (2008). Risk analysis in extended enterprise environments: Identification of critical risk factors in B2B e-commerce relationships. *Journal of the Association for Information Systems*, *9*(4), 160–174. https://doi.org/10.17705/1jais.00155

[51] Guynes, C. S., Wu, Y. A., & Windsor, J. (2011). E-commerce/network security considerations. *International Journal of Management & Information Systems: Second Quarter 2011*, *15*(2), 1–8. clutejournals.com/index.php/IJMIS/article/download/4147/4202

[52] Arden, N. S., Fisher, A. C., Tyner, K., Lawrence, X. Y., Lee, S. L., & Kopcha, M. (2021). Industry 4.0 for pharmaceutical manufacturing: Preparing for the smart factories of the future. *International Journal of Pharmaceutics*, *602*, 120554. www.sciencedirect.com/science/article/pii/S0378517321003598, https://doi.org/10.1016/j.ijpharm.2021.120554

[53] Jajodia, S., Noel, S., Kalapa, P., Albanese, M., & Williams, J. (2011). Cauldron mission-centric cyber situational awareness with defense in depth. In *2011-MILCOM 2011 Military Communications Conference*, 1339–1344. ieeexplore.ieee.org/abstract/document/6127490/

[54] Awasthi, A. (2025). GRC automation in manufacturing modernizing compliance and risk management. *International Journal of Computer Engineering and Technology*, *16*(1), 10-34218.

[55] Alahmari, A., & Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment*, 1–5.

[56] Ali, R. F., Dominic, P. D. D., & Ali, K. (2020). Organisational governance, social bonds and information security policy compliance: A perspective towards oil and gas employees. *Sustainability*, *12*(20), 8576.

[57] Chhetri, I. T. (2022). Cybersecurity and governance, risk and compliance (grc). *Australian Journal of Wireless Technologies, Mobility and Security*, *1*.

[58] Haastrecht, M. van, Sarhan, I., Shojaifar, A., Baumgartner, L., Mallouli, W., & Spruit, M. (2021). A threat-based cybersecurity risk assessment approach addressing SME needs. In *The 16th International Conference on Availability, Reliability and Security*. https://doi.org/10.1145/3465481.3469199

[59] Hubbard, D. W., & Seiersen, R. (2023). *How to measure anything in cybersecurity risk*. USA: John Wiley & Sons.

[60] Jasmontaitė-Zaniewicz, L., Calvi, A., Nagy, R. & Barnard-Wills, D. (2021). *The GDPR made simple (r) for SMEs* (p. 172). Netherlands: ASP Editions-Academic and Scientific Publishers.

[61] Thinyane, M., & Christine, D. (2020). *Cyberresilience in Asia-Pacific* (pp. 12–13, 20–21, 15–17, 79). Japan: United Nations University. collections.unu.edu/eserv/UNU:7760/n2020_Cyber_Resilience_in_Asia-Pacific.pdf

[62] Hoang, D. C., Duc, P. M., & Anh, D. N. (2023). Fostering digital development of small and medium enterprises: A comparison between e-governments of India and Vietnam. *Journal of Logistics, Informatics and Service Science*, *10*(2), 262–280.

How to Cite: Pawar, S., & Palivela, H. (2025). Review and Design of Business Domain-Specific Cybersecurity Controls Framework for Micro, Small, and Medium Enterprises (MSMEs). *Archives of Advanced Engineering Science*. https://doi.org/10.47852/bonviewAAES52024438

APPENDIX A

The following was the questionnaire of the research survey. In these questions, if the participant SME does not have the option to answer in place, they are asked to select "other" in the answer textbox and enter "NA" in the survey.

- Q1. What is the age of your SME?

Purpose: SME representatives are asked to select one of the following options: (i) Less than a year, (ii) Between 1 and 3 years, (iii) Between 3 and 5 years, (iv) Between 5 and 10 years, and (v) More than 10 years. This is because the duration of time that the participating SME exists in the market will allow for a deeper understanding of business maturity with regard to cybersecurity maturity.

- Q2. Are any of the frameworks or standards listed below in use at your organization?

Purpose: Organizations all over the world are adopting a large number of standards and frameworks. The survey offered the option to select from (i) ISO 27001, (ii) PCI DSS, (iii) NIST Cybersecurity Framework (CSF), (iv) HIPAA, (v) FINRA, (vi) GDPR, and (vii) Other in order to determine which of those was adopted by the participating SMEs.

- Q3. Are there security controls in place at your organization?

Purpose: The purpose of the survey was to gather information about any security controls that SMEs have already put in place, regardless of the response to the second question above. The survey offered three answers to this question: (i) Yes, (ii) No, and (iii) Maybe.

- Q4. Please choose PHYSICAL security controls that are already in place.

Purpose: The survey asked participating SMEs to select one or more of the following response options, despite the fact that it is sensitive information for them to reveal which physical controls have been put in place in their company: (i) Fences, (ii) Guards, (iii) Gates, (iv) Access cards, (v) Biometric access controls, (vi) Security badges, (vii) Security lighting, (viii) Surveillance cameras, (ix) Motion sensors, (x) CCTVs, (xi) Fire suppression, (xii) Environmental controls like HVAC and humidity controls, and (xiii) Other. Surveys and other components are among the listed items.

- Q5. Please select the TECHNICAL security controls already implemented.

Purpose: The survey asked participating SMEs to select one or more of the following options: (i) Authentication Solutions, (ii) Firewalls, (iii) Antivirus Software, (iv) Intrusion Detection Systems (IDSs), (v) Intrusion Protection Systems (IPSs), (vi) Constrained Interfaces, (vii) Access Control Lists (ACLs), (viii) Encryption Measures, and (ix) Other.

- Q6. Please select the ADMINISTRATIVE security controls already implemented.

Purpose: The survey asked participating SMEs to select one or more of the following options: (i) security policies; (ii) security guidelines; (iii) security procedures; and (iv) other.

- Q7. How frequently do employees undergo security awareness training?

Purpose: Employee security awareness training aids businesses in being cybersecure in a variety of ways. In order to check it, the survey asked a question with one of the following possible answers: (i) Never; (ii) Once a Year; (iii) Once Every Six Months; (iv) Once Every Three Months; (v) Monthly; (vi) Other.

- Q8. What are the primary concerns you face when deciding whether to implement cybersecurity controls for your company?

Purpose: In order to find out what the biggest issue is with cybersecurity implementation, the survey asked SMEs to select one or more of the following options: (i) Cost of Implementing Cybersecurity Controls; (ii) Uncertain Which Cybersecurity Controls to Implement; (iii) Lack of Resources to Implement and Maintain; (iv) Other business priorities are more important; (v) Lack of a roadmap to invest in cybersecurity control implementation; (vi) Existing cybersecurity standards or frameworks require significant investment; and (vii) Other.

- Q9. Has there been a cyberattack on your company?

Purpose: The survey attempted to find out if SME participants had experienced any cyberattacks since they began their enterprise business journey, in order to gauge the severity of the cyberattack problems. The survey offered three answers to this question: (i) Yes, (ii) No, and (iii) Maybe.

- Q10. Which type of cyberattack was experienced by your company?

Purpose: In response to Q9, the survey asked SMEs to select one or more options to ascertain the type of cyberattack they had experienced: (i) Man-in-the-middle (MITM) attacks, (ii) ransomware, (iii) malware attacks, (iv) web attacks, (v) phishing attacks, (vi) denial-of-service (DoS) attacks, (vii) ransomware, and (viii) other.

- Q11. What do you expect from security frameworks or standards as an SME?

The purpose was to ascertain the SME participants' expectations from cybersecurity frameworks or standards, through an open-ended question.

APPENDIX B

The table below presents the background information of the research survey participants.

Core Business of SME	Participant's Role in SME	SME's Country	Number of Years of SME's Existence
B2C SaaS Hyper Mobility and Fintech consumer services	C-Level Executive	Indonesia	5 to 10
Banking, Financial Services, and Insurance (BFSI)	Director	India	1 to 3
BFSI	Owner/ Partner	India	3 to 5
BFSI	Director	India	More than 10
BFSI	Director	India	1 to 3
Cold Storage & Warehousing	Director	India	More than 10
Construction	Director	India	3 to 5
Construction	Owner/ Partner	India	1 to 3
Construction	Owner/ Partner	Kenya	More than 10
Consulting	C-Level Executive	Ghana	More than 10
Distribution of primary packaging materials	Owner/ Partner	India	More than 10
Distributor	Owner/ Partner	India	1 to 3
E-commerce	Director	United Kingdom	3 to 5
E-commerce	Director	United States	More than 10
E-commerce	Owner/ Partner	India	1 to 3
E-commerce	Owner/ Partner	Russia	Less than 1
E-commerce	Director	India	Less than 1
E-commerce	Director	Australia	More than 10
Education	Vice Principal	India	More than 10
EduTech	C-Level Executive	United States	More than 10
Executive Coaching	Owner/ Partner	United Arab Emirates	3 to 5
Exports	Owner/ Partner	India	More than 10
Finance Services	Owner/ Partner	India	More than 10
Finance Services	Director	India	Less than 1
Finance Services	Owner/ Partner	India	1 to 3
Finance Services	Owner/ Partner	Nigeria	1 to 3
Finance Services	Director	India	Less than 1
Finance Services	Owner/ Partner	Cyprus	More than 10
Finance Services	C-Level Executive	India	More than 10
FMCG	C-Level Executive	India	More than 10
FMCG	Owner/ Partner	India	5 to 10
FMCG	Owner/ Partner	India	Less than 1
FMCG	Owner/ Partner	India	More than 10
Healthcare	Business Unit Head	India	5 to 10
Healthcare	Director	India	1 to 3
Hospitality	Owner/ Partner	India	3 to 5
Hospitality	Owner/ Partner	India	More than 10
Hospitality	Owner/Partner	India	3 to 5
Hospitality	Owner/ Partner	India	More than 10
HR	Owner/ Partner	Norway	Less than 1
Insurance	Owner/ Partner	India	More than 10
Insurance	Owner/ Partner	India	More than 10
IT industry	C-Level Executive	India	5 to 10
IT industry	Owner/ Partner	India	1 to 3
IT industry	C-Level Executive	Russia	More than 10
IT industry	Owner/ Partner	India	1 to 3
IT industry	Owner/ Partner	India	More than 10
IT industry	C-Level Executive	United Arab Emirates	1 to 3
IT industry	Owner/ Partner	India	3 to 5
IT industry	Owner/ Partner	India	More than 10
IT industry	Owner/Partner	Israel	5 to 10
IT industry	C-Level Executive	Australia	5 to 10
IT industry	Owner/Partner	India	More than 10
IT industry	Owner/ Partner	India	Less than 1

(*Continued*)

(*Continued*)

Core Business of SME	Participant's Role in SME	SME's Country	Number of Years of SME's Existence
IT industry	Business Unit Head	Australia	5 to 10
IT industry	Owner/Partner	India	5 to 10
IT industry	Director	United States	5 to 10
IT industry	Director	Singapore	1 to 3
IT industry	Business Unit Head	India	5 to 10
IT industry	Owner/ Partner	India	More than 10
IT industry	Owner/ Partner	India	1 to 3
IT industry	Director	India	5 to 10
IT industry	Director	India	More than 10
IT industry	Director	United States	1 to 3
IT industry	C-Level Executive	India	More than 10
IT industry	Director	India	More than 10
IT industry	Owner/ Partner	India	5 to 10
IT industry	Owner/ Partner	India	Less than 1
IT industry	Director	India	More than 10
IT industry	C-Level Executive	India	5 to 10
IT industry	Owner/Partner	India	1 to 3
IT industry	C-Level Executive	India	1 to 3
IT industry	C-Level Executive	India	3 to 5
IT industry	Director	Ireland	5 to 10
IT industry	Director	United States	3 to 5
IT industry	Director	India	1 to 3
IT industry	Owner/ Partner	India	More than 10
IT industry	Director	India	1 to 3
IT industry	Owner/Partner	India	More than 10
IT industry	Owner/Partner	India	5 to 10
Legal and Accounting Services	Owner/Partner	India	Less than 1
Legal Services	Owner/Partner	India	5 to 10
Logistics	Director	Sweden	3 to 5
Logistics	Owner/Partner	India	1 to 3
Logistics and Supply Chain Management	Director	United Arab Emirates	More than 10
Logistics and Supply Chain Management	Owner/Partner	Bangladesh	5 to 10
Manpower supply (Human resources)	Director	India	5 to 10
Manufacturing	Director	Russia	1 to 3
Manufacturing	Owner/Partner	India	More than 10
Manufacturing	Director	India	More than 10
Manufacturing	Owner/Partner	India	More than 10
Manufacturing	Owner/Partner	India	3 to 5
Manufacturing	C-Level Executive	India	More than 10
Manufacturing	Owner/Partner	India	More than 10
Manufacturing	Owner/Partner	India	More than 10
Maritime	Director	India	1 to 3
Marketing Consultant	Owner/Partner	India	Less than 1
MEDIA	Director	India	More than 10
Media	Owner/Partner	South Africa	Less than 1
Media	C-Level Executive	India	More than 10
MEDIA	C-Level Executive	India	More than 10
Media	Owner/Partner	India	More than 10
Oil Industry	C-Level Executive	United States	More than 10
Online Services and Marketing	Senior Management	Sri Lanka	3 to 5
Online Services and Marketing	Business Unit Head	India	1 to 3
Pharma	Director	United States	More than 10
Pharmaceutical	C-Level Executive	Sweden	More than 10
Renewable Energy	Owner/Partner	India	5 to 10
	C-Level Executive	India	3 to 5

(*Continued*)

(*Continued***)**

Core Business of SME	Participant's Role in SME	SME's Country	Number of Years of SME's Existence
SAAS (Software Development in areas of business process automation for SMB and SME)			
SAS services (Software platform for Insurance brokers)	Director	United States	5 to 10
Telecommunication	Owner/Partner	India	More than 10
Telecommunication	Owner/Partner	India	More than 10
Telecommunication	Owner/Partner	India	3 to 5
Telecommunication	Owner/Partner	India	1 to 3
Travel/Tech	Director	Australia	5 to 10