Toward a Unified Information Security Culture Framework for Small and Medium Enterprises, a Design Science Approach

*Victor Ishola [1], Oluseye Fadiran [2]
[1] Information Systems, Dakota State University, Madison, USA
[2] Computer and Information Science, University of The Cumberlands, Williamsburg, USA
Email: [1] victor.ishola@trojans.dsu.edu, [2] seyetotto@gmail.com

***Abstract*—**Information Security Culture (ISC) research has yielded many competing models and frameworks, each with distinct but related sets of dimensions, elements, and components. This research examines the present state of theoretical frameworks for information security culture, reviews and compares literatures on ISC frameworks, and identifies frequently reoccurring themes, similarities, and gaps specific to small and medium enterprises (SMEs). These gaps are defined by three dynamic capabilities of SMEs organizational resilience namely dynamic absorptive capability (the ability to identify and assimilate external information), dynamic integration capability (the ability to integrate new knowledge with existing functional skills), and dynamic coordination capability (ability to coordinate individual efforts) and three related themes - adaptability and responsiveness of ISC frameworks, integration into daily SME operations, and practicality and ease of implementation. Using design science research methodology (DSRM), a unified but simplified ISC framework aligned with SMEs' three dynamic capabilities as a solution blueprint was developed. The developed artifact is demonstrated by adapting the stages of the generic design process model with elements from the Technology-Organization-Environment (TOE) framework to create a method for adopting and implementing the ISC framework. We assess the unified ISC framework for SMEs based on two key objectives: its alignment with established ISC framework theory and practice as documented in existing literature, and its provision of a clear process for implementation. The paper concludes with a discussion and recommendations for future research

***Keywords*—** *Information Security Culture; Small and Medium Enterprises; Design Science Research; Framework Adoption; Dynamic Capabilities; Security Resilience*

I. PROBLEM IDENTIFICATION AND MOTIVATION

In the contemporary digital landscape, small and medium enterprises (SMEs) are increasingly susceptible to a myriad of information security risks. These risks are not only technological but are profoundly influenced by the organizational culture within which these technologies are embedded. An area that has been identified as significantly underserved in both academic and practical contexts is the development of a robust Information Security Culture Framework specifically designed for SMEs. This necessity stems from 1) the fact that extant research in information security culture has yielded many competing models and frameworks with each framework having different but related sets of dimensions, elements, and components leaving the SMEs inundated with information, the analysis to select a single or best of breed framework with the shortest possible path to implementation and value that aligns with their dynamic capabilities [1] 2) the persistent challenges SMEs face in securing their informational assets, a predicament that is exacerbated by their limited resources compared to larger enterprises [2], [3].

The relevance of this problem is underscored by the dramatic increase in cyber threats targeting SMEs, whose often inadequate security measures make them attractive targets for cybercriminals [4], [5]. Approximately 1.6 million small businesses fall prey to cyber-attack [6]. Research suggests that while technological solutions are readily available, their effectiveness is significantly compromised without a strong underlying security culture [7]. Therefore, enhancing the information security culture within SMEs is not only a matter of developing frameworks but also involves ensuring those frameworks are aligned with the dynamic capabilities [1] of SMEs to foster adoption and ultimately improve their security posture.

SMEs play a vital role in driving economic growth, innovation, and employment opportunities in various industries worldwide. They often exhibit characteristics such as flexibility, adaptability, and entrepreneurship, which enable them to respond quickly to market changes and opportunities. SMEs face unique challenges related to resource and financial constraints, limited expertise/skills, technology adoption, and scalability, which require tailored strategies and support measures to enhance their competitiveness and sustainability [8], [9], [10].

The motivation for addressing this problem is twofold. First, there is a critical business imperative to protect organizational assets from increasing cyber threats. Second, there is an academic and practical gap in how information security culture frameworks are tailored specifically to the needs and constraints of SMEs [11], [12]. Many existing

Received: 1-08-2024
Revised: 11-09-2024
Published: 21-09-2024

frameworks are designed with larger organizations in mind, often requiring resources and scale that SMEs do not possess.

Reference [1] identified dynamic capabilities and demonstrated their impact on organizational resilience for SMEs. Their findings revealed that the dynamic integration capability had the weakest influence on SMEs' organizational resilience. We argue that despite SMEs generally excelling in dynamic detection capabilities—such as identifying changes in the IT security landscape—they often fall short in dynamic absorptive capability (the ability to identify and assimilate external information), dynamic integration capability (the ability to integrate new knowledge with existing functional skills), and dynamic coordination capability (coordinating individual efforts). The ability of SMEs to leverage emerging digital technologies and technology best practices has a moderating effect on the significance of the role that SMEs play in the domestic and global economy. What good is having a framework or new information that is supposed to help you improve but can't because the complexity of the new information is too much for your organization's dynamic capability? This disconnect underscores the need for a framework that not only addresses the unique challenges faced by SMEs but also leverages their nimble and innovative capabilities.

II. Solution Objectives

The objective of this research is to develop and evaluate a framework that SMEs can leverage to improve information security culture in their organization using a Design Science Research (DSR) approach. This approach is particularly suited for this type of research as it allows for the iterative development and refinement of artifacts based on real-world application and feedback [13]. *The research hypothesis proposed in this study (see Figure 1) is that if a tailored information security culture framework is developed for SMEs, the dynamic absorptive, integration, and coordination capability will positively improve, leading to better adoption of the security culture framework and ultimately enhancing the overall security posture of the organization* [1], [14], [15]. The research question that guides this inquiry is: How well does a tailored Information Security Culture Framework effectively enhance the intention to adopt the framework, security behaviors, and policy compliance within SMEs*?*

This study employs the DSR methodology to create a unified, practical, actionable framework that SMEs can implement to cultivate a stronger information security culture. This methodology involves the construction and evaluation of the framework through descriptive and static analysis. By focusing on the specific needs and constraints of SMEs, this study aims to contribute significantly to the existing body of knowledge by providing a nuanced understanding of how an information security culture can be effectively developed and sustained in this crucial segment of the economy.

III. Artifact Design and Development

A. Search Strategies

The design of effective artifacts requires the execution of a rigorous search process [16]. A comprehensive literature search method is essential in developing a strong Information Security Culture Framework customized for SMEs. Our strategy included two parts. The first literature search and review were intended to identify the problem and characterize the problem area, with an emphasis on the specific information security challenges that SMEs face, [17], [18], [8], [9], [10]. The second literature search and review were conducted to find a suitable solution space and design artifact for the problem, ensuring that the suggested framework is informed by best practices and successful information security measures [19], [20]. This dual approach allowed for a thorough understanding of both the challenges and potential solutions, resulting in the development of a well-rounded and unified framework that meets the objectives of this research. The literature review focused on academic databases like IEEE Xplore, ABI/INFORM, Google Scholar, Springer, and the ACM Digital Library, see Figure 2. These sources were chosen for their wide range of peer-reviewed articles, conference papers, and books covering information technology, cybersecurity, and organizational behavior. Only publicly available or Dakota State University library-accessible literature in English was included

The search query comprised two parts, both refined through pilot searches. The first was used to identify studies related to information or cyber security culture frameworks while the second located studies with an emphasis on SMEs. The search employed a combination of keywords and phrases to ensure thorough coverage of the subject. Keywords included "Information security culture framework," "cybersecurity culture," "SMEs and information security culture," "Information security culture model," and "organizational culture and information security". This approach aimed to capture both broad overviews and specific studies pertinent to the development of security culture within SMEs.

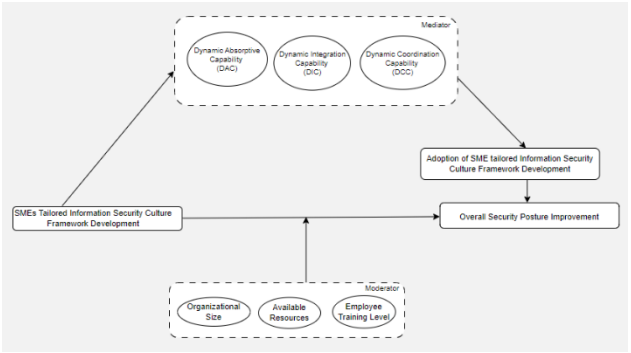

Fig. 1. Research Hypothesis

The screening phase was divided into two parts. The first involved the assessment of study titles and abstracts, while the second involved a full-text review. Inclusion criteria were set to consider only peer-reviewed publications from the last eight years (2015 – 2023) that explicitly addressed aspects of information security within SME contexts or provided insights into security culture frameworks in general. This is to ensure the relevance of the literature reviewed to today's SMEs' organizational and technological context. Exclusion criteria filtered out articles not directly contributing to the understanding or development of security culture frameworks.

Throughout the review process, the search strategy was periodically evaluated and adjusted. Initial searches were

broad to ensure a wide capture of relevant literature, returning a total of 390 articles from the initial search criteria before refining the search terms [21], [11].

B. Current Approaches and Outcomes of Information Security in SMEs

A systematic review of small and medium-sized enterprise (SME) cybersecurity literature points out important issues. These include the fact that current recommendations are often too theoretical or complicated for SMEs to put into practice. SMEs would benefit from a cybersecurity measurement framework tailored to their needs. Challenges related to human factors and managing cyber risks in SMEs are not adequately addressed. Existing Information Security Management Frameworks (ISMF) do not provide enough guidance specific to SMEs. SMEs need more flexible and practical solutions that consider their limitations, such as limited expertise, complexity, infrastructure, organizational changes, and financial constraints [22]

Databases	Information Security in abstract, 2015-2023, English				
	#Records identified through database searching	#Records after duplicates removed	#Records screened	#Records excluded (exclusion/inclusion criteria)	#Full text articles assessed for eligibility
IEEE Xplore	100	90	91	41	50
ABI/Inform	100	95	93	37	56
ACM Digital Library	90	96	90	40	50
Google Scholar	70	60	58	18	40
Springer	30	26	23	3	20

Fig. 2. Summary of Literature Search

Furthermore, literature suggests that while some SMEs are becoming increasingly aware of the necessity for robust information security measures, many continue to struggle with implementation due to resource constraints, budget constraints, a lack of specialized knowledge, complexity of security solutions, perception of low risk, and a lack of regulatory pressure [23], [2], [24], [25], [26], [27], [28], [29], [30], [66]. This divergence in capability and practice underpins much of the current discussion in the field, highlighting a critical gap between knowledge and practice.

The ongoing dialogue in the literature suggests that while progress has been made, significant work remains to develop security practices that are both effective and manageable for SMEs. Existing research has identified numerous significant aspects influencing technology adoption, adaptation, and compliance in SMEs, emphasizing the need for specialized solutions. For example, [31], [32], [33] emphasize the necessity of flexibility and scalability in technology solutions for SMEs, citing their changing operational contexts and limited IT resources and capability. By addressing these specific needs and limits, the proposed framework intends to provide a potentially useful tool in the attempt to improve SMEs' security postures sustainably.

C. Information Security Culture Frameworks

Various frameworks have been suggested to promote a strong information security culture. These frameworks typically advocate for a comprehensive approach that combines organizational, environmental, technological, and behavioral aspects to establish a secure environment. For example, [12] proposes a framework that incorporates policy, education, and technology to encourage security-conscious behaviors among employees. Similarly, [34] has introduced models that integrate creativity and innovation into building a security culture, highlighting the importance of involving employees in security practices for sustainable compliance.

These frameworks often include components such as regular security training, clear communication of security policies, involvement of top management, and the implementation of technical controls [35], [36]. A comparison of these frameworks reveals that while all aim to enhance security practices, their applicability and effectiveness can vary significantly. Some frameworks focus heavily on behavioral change through training and awareness programs, whereas others emphasize the strategic alignment of security practices with business objectives [13].

Ongoing challenges remain in developing information security culture frameworks for SMEs. Debates in the literature focus on the balance between behavioral and technical approaches, the scalability of frameworks to accommodate growth and change, and the integration of new technologies into existing security practices. These discussions highlight the continuous need for research that addresses these evolving challenges, ensuring that SMEs can not only establish but also maintain an effective security culture amidst changing organizational and technological landscapes [37], [25].

D. Literature Gaps Identified

A systematic analysis of the existing literature on Information Security Culture (ISC) frameworks revealed numerous notable gaps, especially in their relevance to small and medium-sized organizations (SMEs), see Figure 3. To begin, the assessment identified a common issue: most ISC frameworks are created with large enterprises in mind and do not sufficiently meet the unique demands and limits of SMEs. For example, [38] discovered that many frameworks presume the availability of significant resources, both financial and human, which SMEs frequently lack. Similarly, [39] noted that SMEs often have fewer funds and fewer specialized IT security workers, making it harder to establish complete security controls.

Second, the review found a significant lack of empirical validation of ISC models/frameworks, particularly in the SME environment. Many existing frameworks are theoretical, with insufficient practical, real-world adoption to demonstrate their usefulness. The intricate nature of existing information security culture frameworks often hinders their practical application in SMEs. Their complexity, coupled with visual representations, can be overwhelming, discouraging implementation. Reference [40], [41], [42] adopted and applied existing ISC framework to SMEs, academia and MITRE ATT&CK risk context respectively. However, the most prominent application is from the evaluation phase of the study that created the framework where the utility, relevance, and efficacy of the study's proposed framework are conducted. Although one case study research on ISC model was found [43] however it was excluded from our review and synthesis as it was written in a language other than English, hence it did not meet the inclusion criteria for our literature search and review. The lack of case studies or action research using existing ISC frameworks indicates low adoption and implementation of

these conceptual frameworks in practice, which we argue is partly owing to the perceived lack of alignment of the framework design with organizations' dynamic capabilities.

Thirdly, the literature review highlighted a heavy emphasis on behavioral research paradigms for developing information security culture (ISC) frameworks, with no study employing design science research methodology, see Figure 3. The reviewed research often focused on generic or non-SME contexts, highlighting the need for a framework specifically tailored to Small and Medium Enterprises (SMEs), since ISC must be contextualized. Existing ISC framework dimensions tend to be too broad for SMEs, suggesting a need for more streamlined and context-specific models. Additionally, while some studies labeled their work as assessments, they were often focused on developing new frameworks rather than evaluating existing ones, aligning with the exclusion criteria for this review.

These gaps suggest the need for a more unified approach that considers the interplay between technology, policy, human behavior, communication, dynamic capabilities, and limitations in the security landscape of SMEs. Figure 3 provides a selected but related overview of previous research on information security culture frameworks, including identified gaps.

E. Theoretical Basis

Theoretical foundations in information security culture for small and medium enterprises (SMEs) draw mainly from organizational behavior theories emphasizing the importance of shaping attitudes and behaviors towards security [2], [12]. The Theory of Planned Behavior [44] and Security Culture Framework [45] offer insights into individual behaviors and organizational culture's role in information security practices within SMEs. Cultural Theory of Risk [46] and Organizational Culture Theory [15] provide valuable perspectives on how cultural values and organizational norms influence security practices These theories suggest that security behaviors are not just the result of individual awareness but are also significantly influenced by the broader organizational culture and the prevailing security norms within it.

The ongoing development of theoretical models in information security culture for SMEs should focus on practical application and adaptability to real-world contexts [36]. To achieve this, we adopt the three major stages of the generic design process models as the first theoretical basis for the ISC framework designed and proposed in this study. The 3 stages are analysis (how it is today/current state), projection (how it could be/the ideal future state), and synthesis (how it is tomorrow) [47]. During the Analysis stage, current practices reveal that SMEs confront significant obstacles due to resource restrictions, a lack of specialized knowledge, and evolving cyber risks. The Projection stage describes an ideal state in which security procedures incorporate technological, behavioral, and cultural measures to promote continual development and flexibility [35], [36]. Finally, the Synthesis step integrates these insights to create a personalized framework that targets SME-specific needs, offers realistic adoption guidance, and responds to dynamic threats, hence improving SMEs' security posture over time [37].

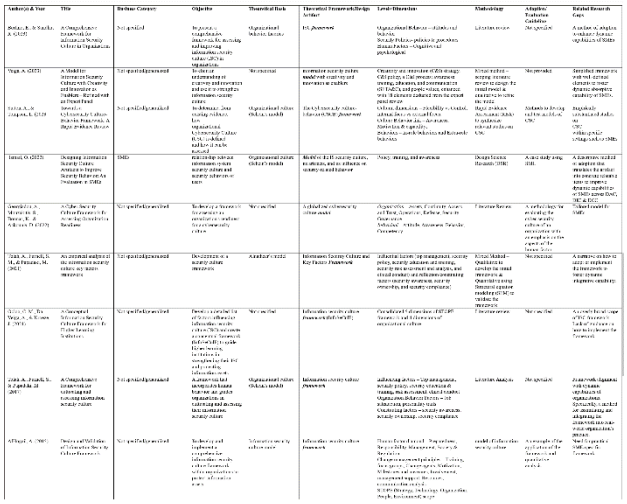

Fig. 3. Selected Previous Studies on Information Security Culture Frameworks

The second theoretical basis adopted for this research is the organizational resilience model for SMEs with dynamic capabilities dimensions of absorption, integration, and coordination. Dynamic Absorptive Capability (DAC) is the ability to identify and assimilate external information in a manner that it can be utilized to achieve set objectives. Dynamic Integration Capability (DIC) is the efficient combination and integration of the newly acquired knowledge with routine activities and existing functional skills within the organization. It is also the ability to leverage an opportunity once identified and absorbed in response to the environment. Dynamic coordination capability (DCC) is the ability to coordinate, make timely adjustments, and synchronize internal processes and resources to facilitate rapid reconfiguration

The Unified Theory of Acceptance and Use of Technology (UTAUT) is adapted and serves as the third theoretical basis. UTAUT, proposed by [48], integrates elements from various models and includes performance expectancy, effort expectancy, social influence, and facilitating conditions as key determinants of technology adoption. Within the realm of UTAUT, we consider only performance expectancy (the degree to which the SME organization believes using the framework will help attain improvement of ISC in the organization), effort expectancy (the degree of ease associated with the use of the framework, measured by perceived ease of use, and complexity) and facilitating conditions (the degree to which existing organization processes and infrastructure supports the use of the framework, measured by compatibility) relevant to this study.

Design Science Research (DSR) is about creating a future reality with a specific purpose in mind [49]. This research paradigm emphasizes iterative development, enabling researchers to refine their frameworks or models through cycles of creation, testing, evaluation, and refinement. Such an approach is essential when addressing complex problems like information security, where theoretical models must be continuously adapted to meet the evolving technological and human factors [13]. DSR's applicability to this study is further justified by its ability to bridge the gap between theory and practice. It not only supports the development of

theoretical knowledge but also stresses the importance of creating tangible, actionable outcomes that directly benefit practitioners—particularly vital for SMEs, which often lack the resources to engage in extensive theoretical explorations without immediate practical implications [36]. The iterative nature of DSR allows for the incorporation of feedback from SME stakeholders, ensuring that the resulting information security culture framework is both relevant and effective in a real-world setting

F. Artifact Design

Design science creates and evaluates IT artifacts that solve problems identified in an organization [16]. Given that design is a search process, the proposed framework addresses the gaps identified in the literature. For this study, the model-type artifact that the unified ISC (Information Security Culture) framework represents is in accordance with the constructs and models category of artifact types. It is a model composed of terms, abstractions, and representations that together characterize the ideas, connections, and components necessary to support a strong information security culture in Small and Medium-Sized Businesses (SMEs) [16]. The framework defines aspects that are critical for fostering a culture of security awareness and compliance, including organizational policies, employee behaviors, communication channels, and technological interventions [34]. The proposed framework, developed through abstraction and representation that facilitates comprehension of the intricacies of information security in SME contexts, is conceptualized as a multi-component model that addresses core dimensions of information security culture. The entire framework can be divided into two parts, the flexible component (which is the upper half) and the flexible entry/starting point phases (which is the lower half). The component of our framework is described here and represented graphically in Figure 4.

Policy Development and Implementation: Reference [50] found a positive relationship between security policy and security culture. Reflecting insights from [51], [3], [52], [53], [40], this aspect of the framework focuses on the creation of clear, concise security policies that are well communicated and enforced, with specific adjustments to accommodate the flexibility required by SMEs. It also includes establishing supporting procedures and guidelines required to enforce policy and address non-compliance. For example, a policy mandating password updates and specifying acceptable password practices.

Technology and Tools: Informed by [54], this component involves the integration of appropriate technological solutions/technical controls that align with, and enable the security policies, needs, and operational practices of SMEs, ensuring that security enhancements do not hinder business operations. For example, implementing a multi-factor authentication system to support the Access Control policy to enhance the protection of sensitive information, or implementing a password manager allows users to create and store strong, unique passwords for all their accounts. This eliminates the need to remember complex passwords or reuse them across multiple platforms, reducing the risk of breaches.

Awareness and Training: Two of the findings that emerged from SMEs cybersecurity systematic literature review are the themes “risk awareness improves cybersecurity behaviors”, and “top priority should be given to initiatives focused on improving the organization’s cybersecurity awareness” [22]. According to [53], a notable deficiency in the Information Security Culture (ISC) of Small and Medium Enterprises (SMEs) is the absence of security education, training, and awareness (SETA) programs. While evaluating the influence of key components of a comprehensive information security program, [55] found that Security Education Training and Awareness (SETA) programs significantly influence security culture and employees' awareness of security policies. Reference [2] extended Schein’s model by adding a fourth layer, the knowledge layer. Reference [12] found a positive relationship between knowledge, security behavior, and culture. This component of the proposed ISC framework for SMEs emphasizes empowering employees through augmented knowledge sharing and communicating the vital connection between business processes, technical processes, and cybersecurity. Building on the work of [35], this component leverages the use of engaging and interactive methods such as gamification and others to communicate policies and improve security compliance behavior. By making learning processes more engaging, SMEs can enhance their employees' understanding and retention of critical security practices. For example, performing regular phishing simulation exercises to raise awareness and help improve employee behavior regarding phishing.

Behavior Management: Introducing a security culture in an organization involves changing human behavior gradually. This change can be broken down into three parts: a stimulus or trigger, routine actions, and a reward. Employees need to want, know, and be able to adopt this culture. Providing strong support and motivation is crucial to encourage employees to develop positive habits, share knowledge, and act in line with the organization’s cybersecurity values [56]. By offering regular feedback, reinforcement [7], and rewards, SME organizations can promote proactive security behaviors and create a collective sense of responsibility for security among employees. For instance, recognizing and rewarding employees who actively contribute to improving cybersecurity knowledge and practices within the organization

Adaptation and Continuous Improvement: Reference [23] identified security analysis, improvements and communications as areas needing more work for SMEs cybersecurity. Echoing the principles of DSR, this component underscores the need for ongoing evaluation and adaptation of the security framework to address emerging threats and changes within the business environment [11], [37]. For example, annual updates to security programs and initiatives based on audit findings. The audit could be internal or external. To ensure the sustainability and continuous improvement of the framework, a feedback loop is integrated into its design. This loop involves regular reviews and updates to the framework based on emerging security threats, technological advancements, and feedback from users. Such a mechanism is critical in maintaining the relevance and effectiveness of the framework over time, adapting to changes in the security landscape and business practices of SMEs [11]. This phase may require the infusion of program

management and change management practices for successful adoption [57].

In grounding the problem framing in reality and developing the framework for fostering an information security culture in SMEs, this research draws upon a rich body of theoretical and empirical literature, then applied disciplined imagination, idealized design and abductive reasoning [49]. Each component of the framework is designed to be modular yet interconnected, allowing SMEs to implement the model progressively and tailor it to their specific contexts and needs. The construction of this model leverages a range of empirical data and expert input, ensuring its foundation is robust and its applications are validated through iterative testing and refinement. This process not only helps in fine-tuning the framework to increase its efficacy but also ensures it is versatile enough to be adapted across different SME contexts, thereby broadening its applicability and impact

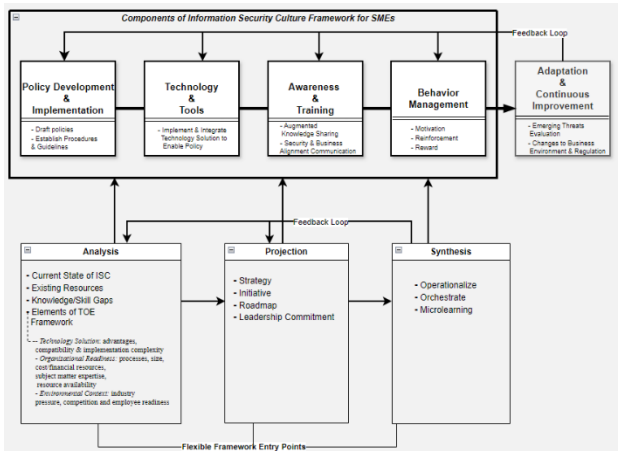

Fig. 4. Unified Information Security Culture Framework for SMEs

IV. DEMONSTRATION

The overarching objective of demonstrating and evaluating the proposed unified ISC framework, the design artifact, is to ensure the framework aligns with the three dynamic capabilities of absorption, integration, and coordination, as well as adequately addresses three themes that emerged from the gaps identified for SMEs in extant literature regarding ISC frameworks, namely – 1) adaptability and responsiveness in ISC frameworks, 2) integration into everyday operations of SMEs, and 3) practicality and implementation ease. We demonstrated the proposed unified Information Security Culture (ISC) framework by adapting, extending and combining the generic design process model stages [47] with some elements of the Technology-Organization-Environment (TOE) framework [58] to develop a new method or nominal process of adopting and implementing the ISC framework.

We addressed the adaptability dimension of the first theme by ensuring components of the framework are informed and driven by key gaps and core aspects of information security culture identified in extant literature [2], [34]. The responsive dimension of the first theme was addressed by ensuring the framework is modular with flexible starting components and entry points, both of which are informed by tacit knowledge and expert judgment of the specific SME context. The framework was designed to be flexible enough to adapt to evolving cyber threats, reflect changing regulations, scale up or down as the SME organization grows or shrinks, accommodate different SMEs' needs, and integrate with existing processes and current practices [59], [60].

The second theme was addressed by ensuring the modular framework allows for a phased approach with actions, programs, or initiatives that fit seamlessly into and complement existing workflows, and everyday operations without creating significant disruptions, drastically altering daily operational routines, or hindering productivity, this aligns with the dynamic integration capability (DIC) and dynamic coordination capability (DCC) dimensions of SMEs [61], [62].

The third theme was addressed by ensuring the framework is simple to understand even for an entry-level IT or cybersecurity practitioner and it is focused on the most critical areas needed to create a security culture while maximizing impact with limited resources. This aligns with the dynamic absorptive capability (DAC) dimension of SMEs. The implementation ease dimension of the third theme also ties to the adaptability and responsiveness of the first theme. Each module of the framework is designed to be independently implemented facilitating adaptability to varying organizational SME contexts. However, flexibility in implementation does not imply arbitrary selection or random ordering of components. Rather, it allows organizations to prioritize modules based on their specific needs and readiness levels while ensuring coherence and alignment with overarching security objectives. The conceptual representation of the framework and its narrative will elucidate interdependencies among components, delineating hard dependencies where applicable. This approach aligns with best practices in framework design, which emphasize both modularity and logical sequencing to maximize effectiveness and relevance [63], [64], allowing SMEs to adopt the framework in stages according to their specific needs and capacities. This modular approach not only makes the framework more accessible for smaller enterprises but also facilitates focused testing and refinement of each component.

The generic design process model includes three stages: Analysis, Projection, and Synthesis. In this context, the Analysis stage requires the SME to evaluate the current state of security culture and determine the specific needs and constraints. The objective is to comprehend the organization's existing security posture, resources, and skill gaps across all four components of the proposed ISC framework.

To conduct the Analysis phase, we employ selected components of the Technology-Organization-Environment (TOE) framework [58]. This involves assessing the Technology context, which considers the advantages, compatibility, and complexity of implementing a given internal/external technology solution when compared to the current state, within the context of enabling and supporting organizational policies towards improving overall security culture. The second component is the Organizational context, which assesses the organization's readiness in terms of processes, size, cost/financial resources, subject matter expertise, and resource bandwidth availability. Lastly, the

Environmental context evaluates the industry pressure/competition and employee readiness.

During the Projection phase, the SME designs a strategy that selects and prioritizes components of the proposed ISC framework to address the critical elements of capabilities and needs identified during the Analysis phase. Since the ISC framework is designed to be modular and components can be implemented in any order, the SME creates an implementation roadmap, which is essentially an initiative with high-level actionable steps and timelines for implementing each component of the proposed ISC framework with allocated resources. This phase may require the involvement and commitment of the organization's leadership to the developed strategy. Lastly, the Synthesis phase is extended with a feedback loop. It involves the operationalization and orchestration of the output from the Projection phase. This is where the SME fully executes the program's practical steps and schedules, which were determined in the earlier (projection) phase. The feedback loop carries the microlearning to the analysis and projection phases.

A. Scenario-Based Implementation Method

In a scenario where a small to medium-sized enterprise (SME) wants to apply the ISC framework. The SME's subject matter expert (SME), based on tacit knowledge of the organization and expert/professional judgment, starts by analyzing the policy development and implementation within the organization. The objective is to understand the current security culture, available resources, knowledge and skill gaps, and specific needs and limitations for the policy development & implementation component.

The SME evaluates whether existing policies effectively promote better security behavior, this aligns with the organizational context of the TOE framework. For instance, the analysis could reveal that multi-factor authentication is not required for accessing sensitive information due to lack of appropriate access control policies or inadequate technology to support and enable existing access control policy. If the latter is identified as root cause, the analysis will include assessing a technological solution to enable an existing access control policy, considering its advantage, compatibility with existing solutions, and the complexity of its implementation. This evaluation corresponds to the Technology context of the TOE framework. The analysis may loop back to the organizational context to consider factors like cost, resource availability, and implementation time. Next, the SME examines the environmental context, assessing employee readiness, policy knowledge, skill gaps, competitive advantage, and intention to comply with policies. This informs components such as Awareness & Training and Behavior Management.

After completing the analysis for the selected component, the SME moves to the projection phase, establishing strategy, actions, and timelines to address identified gaps and obtain senior leadership approval. For example, creating initiative and roadmap to develop a new access control policy, procedures, and guidelines to enforce them company-wide, or implement suitable technology solutions to support policy compliance.

Finally, in the synthesis phase, the proposed strategy is implemented within the specified timeline. This process is iterative, employing the feedback loop that exist at both the ISC framework components level and the entry point phases, allowing the SME to cycle through analysis, projection, and synthesis multiple times until all components of the ISC framework are addressed and valuable input is provided.

V. EVALUATION

Reference [16] enumerated five design evaluation methods, namely, observational, analytical, experimental, testing, and descriptive. We adopt both the analytical (specifically, static analysis that examines the structure of artifacts for qualities such as complexity), and descriptive (information from knowledgebase and scenarios) as primary evaluation methods for this research. Since our objective is to design a unified but simplified ISC framework that is aligned with the three dynamic capabilities of SMEs as a solution blueprint, in contrast to the many competing models and frameworks that exist currently with each framework having different but related sets of dimensions, elements and components. From an analysis standpoint, we assess the structure of the unified ISC framework artifact proposed in this study as streamlined, straightforward, and comprising of core elements from previous frameworks. These characteristics will further improve the three dynamic capabilities of SMEs thereby leading to more adoption. From a descriptive evaluation standpoint, following [65], we evaluate the unified ISC framework for SMEs as described above in terms of two objectives. First, is it consistent with prior ISC framework dimensions, elements, and theory as represented in literature? Second, does it provide a nominal process for implementing the framework?

First, the unified ISC framework is consistent with artifacts in prior literature about ISC frameworks. We can verify this by referring to our analysis in figure 3. [12], [68] is far more general in its objectives than this current research, however, some dimensions of its framework such as training, motivation, and communication can be mapped roughly to the unified ISC framework. [13], [36], [50], [67], [70] are all consistent with the unified ISC framework for SMEs.

Secondly, the unified ISC framework provides a nominal process for creating a culture of information security in SMEs following the detailed, scenario-driven method described for implementing the ISC framework in SMEs in the demonstration section of this study.

VI. CONTRIBUTIONS AND FUTURE RESEARCH

A. Contributions

This research undertaken to develop an Information Security Culture Framework specifically for small and medium enterprises (SMEs) represents a significant step forward in addressing the unique challenges and needs of this crucial sector. The originality of this research lies in its methodological approach and its focus. By applying the Design Science Research (DSR) methodology, the study not only contributes a novel artifact to the field but also enhances the body of knowledge concerning the integration of security culture within the operational and strategic frameworks of SMEs – an example of a new solution to old problems [49].

The originality of the research can be further delineated through its focus on SMEs—a group often underserved in information security research, which tends to focus either on individual behavior or large organizations. This focus is

crucial because SMEs face distinct challenges such as limited resources, lack of specialized knowledge, and higher vulnerability to cyber threats due to less sophisticated security measures [25]. By streamlining existing frameworks and tailoring it specifically for SMEs, this research addresses a significant gap in the current literature and provides a practical, scalable tool that can be directly applied within these organizations to foster a security culture. In design science (DS), theoretical contributions focus on creating new or improved action blueprints for addressing challenges, rather than providing explanations for existing empirical facts. DS studies aim to generate new facts instead of reconciling discrepancies in existing data [49], accordingly, this research contributes to the adoption and implementation of ISC frameworks by providing a detailed scenario-driven step-by-step implementation method that SMEs can follow to implement and adopt the framework so that they are not inundated with how to adopt the framework

B. Limitations & Future Research

This study is limited in the sense that the proposed ISC framework is a conceptual framework though its components provide a solution to the challenges associated with selecting, and implementing ISC frameworks, and cultivating ISC in SMEs, hence in future work, we will perform a semi-quantitative questionnaire-based survey that combines a Likert scale with a qualitative comments section. This approach enables us to capture both the overall perception of the framework and gain valuable insights into the rationale behind those perceptions. This method can be especially beneficial for tailoring the framework for better adoption in resource-constrained SME environments. We'll conduct a case study or action research to further evaluate the framework using expert reviewers (Information Technology and Security professionals in Small and Medium Enterprises) to demonstrate the utility (relevance), quality, and efficacy of the ISC framework and customize it further to the context of SMEs. A case study allows for a detailed examination of the implementation process and the impact of the framework within a single SME. This can provide valuable insights into the real-world challenges and successes of implementing the framework. Furthermore, future research can improve rigor in validation by employing a comparative, quasi-experimental study design, which will involve implementing the framework in a sample group of SMEs (intervention group) and comparing their pre- and post-implementation security posture with a control group of SMEs that do not implement the framework. This control group helps in establishing a clearer causal relationship between the introduction of the framework and observed changes in security culture and compliance. Such a design not only strengthens the validity of the research findings but also provides a more compelling narrative for the framework's effectiveness to stakeholders and potential adopters.

REFERENCES

[1] V. M. García-Valenzuela, C. Jacobo-Hernandez, and J. G. Flores-López, "Dynamic Capabilities and their Effect on Organizational Resilience in Small and Medium-Sized Commercial Enterprises," Management & Marketing, vol. 18, no. 4, pp. 496-514, 2023. doi: https://doi.org/10.2478/mmcks-2023-0027

[2] J. F. Van Niekerk and R. Von Solms, "Information security Culture: A Management Perspective," Computers & Security, vol. 29, no. 4, pp. 476-486, 2010. doi: https://doi.org/10.1016/j.cose.2009.10.005.

[3] M. Sadok, S. Alter, and P. Bednar, "It is not my job: Exploring the Disconnect between Corporate Security Policies and Actual Security Practices in SMEs," Information & Computer Security, vol. 28, no. 3, pp. 467–483, 2020. doi: https://doi.org/10.1108/ics-01-2019-0010

[4] J. Smith and A. Johnson, "Cybersecurity for Small and Medium Enterprises: A Comparative Analysis," Journal of Small Business Management, vol. 57, no. 3, pp. 451-469, 2019

[5] M. Garcia and R. Martinez, "Trends and Challenges in Cybersecurity for Small and Medium Enterprises," International Journal of Business and Social Science, vol. 9, no. 2, pp. 98-115, 2018

[6] H. Jahankhani, L. N. K. Meda, and M. Samadi, "Cybersecurity Challenges in Small and Medium Enterprises (SMEs)," in Blockchain and Other Emerging Technologies for Digital Business Strategies, Springer, 2022, pp. 1-20

[7] B. Uchendu, J. R. Nurse, M. Bada, and S. Furnell, "Developing a Cyber Security Culture: Current Practices and Future Needs," Computers & Security, vol. 109, p. 102387, 2021. doi: 10.1016/j.cose.2021.102387

[8] S. K. Naradda Gamage et al., "A Review of Global Challenges and Survival Strategies of Small and Medium Enterprises (SMEs)," Economies, vol. 8, no. 4, p. 79, 2020. doi: 10.3390/economies8040079

[9] A. Telukdarie, T. Dube, M. Munsamy, K. Murulane, and R. Mongwe, "Navigating Digital Challenges for SMEs: A Two-Tier Approach to Risks Mitigation and Sustainability," Sustainability, vol. 16, no. 14, p. 5857, 2024. doi: 10.3390/su16145857

[10] R. Pérez Estébanez, "An Approach to Sustainable Enterprise Resource Planning System Implementation in Small- And Medium-Sized Enterprises," Administrative Sciences, vol. 14, no. 5, p. 91, 2024. doi: 10.3390/admsci14050091.

[11] A. Mahfuth, S. Yussof, A. A. Baker, and N. A. Ali, "A Systematic Literature Review: Information Security Culture," in 2017 International Conference on Research and Innovation in Information Systems (ICRIIS), Langkawi, Malaysia, 2017, pp. 1-6. doi: 10.1109/icriis.2017.8002442

[12] A. AlHogail, "Design and validation of information security culture framework," Computers in Human Behavior, vol. 49, pp. 567–575, 2015. doi: 10.1016/j.chb.2015.03.054

[13] S. G. Govender, M. Loock, E. Kritzinger, and S. Singh, "Using Design Science Research to Iteratively Enhance Information Security Research Artefacts," in Computer Science On-line Conference, Cham: Springer International Publishing, 2023, pp. 49-61. doi: 10.1007/978-3-031-35317-8_5

[14] D. Lacey, "The Art of Information Security Culture," Information Security Journal: A Global Perspective, vol. 30, no. 4, pp. 191-202, 2021. doi: 10.1080/19393555.2021.1931792

[15] E. H. Schein, Organizational Culture and Leadership, 4th ed., Jossey-Bass, 2010

[16] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science in Information Systems Research," MIS Quarterly, vol. 28, no. 1, pp. 75–105, 2004. doi: 10.2307/25148625

[17] A. Smith and J. Brooks, "Understanding Cybersecurity Challenges in Small and Medium-sized Enterprises (SMEs)," Journal of Small Business Management, vol. 59, no. 3, pp. 227-247, 2021. doi: 10.1080/00472778.2021.1935760

[18] M. Alshaikh, "Developing cybersecurity culture to influence employee behavior: A practice perspective," Computers & Security, vol. 98, p. 102003, 2020. doi: 10.1016/j.cose.2020.102003

[19] E. Johnson, S. Goel, and S. Misra, "Best Practices in Cybersecurity: Building Effective Security Cultures in SMEs," Journal of Cybersecurity, vol. 8, no. 1, p. tyac006, 2022. doi: 10.1093/cybsec/tyac006

[20] T. A. Nguyen and X. Luo, "Enhancing Information Security Behaviors in SMEs: A Comprehensive Framework," International Journal of Information Management, vol. 61, p. 102369, 2021. doi: 10.1016/j.ijinfomgt.2021.102369

[21] T. Oliveira, M. Thomas, G. Baptista, and F. Campos, "The impact of organizational factors on information security policy compliance: A multi-case study," Journal of Information Security and Applications, vol. 58, p. 102646, 2021. doi: 10.1016/j.jisa.2021.102646

[22] C. R. Junior, I. Becker, and S. Johnson, "Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity," arXiv preprint arXiv:2309.17186, 2023. doi: 10.48550/arXiv.2309.17186

[23] A. Chidukwani, S. Zander, and P. Koutsakis, "A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations," IEEE Access, vol. 10, pp. 85701-85719, 2022.

[24] E. Etim and A. Anand, "Cyber Security Practices in Small and Medium Enterprises: A Study of Nigeria," International Journal of Engineering and Advanced Technology, vol. 8, no. 5, pp. 3281-3285, 2019

[25] K. A. Saban, S. Rau, and C. A. Wood, "SME executives' perceptions and the information security preparedness model," Information & Computer Security, vol. 29, no. 2, pp. 263-282, 2021. doi: 10.1108/ics-01-2020-0014

[26] A. Dumitraşcu and C. N. Ciocoiu, "Cybersecurity Awareness in Small and Medium-sized Enterprises: A Romanian Perspective," Economics, Management and Financial Markets, vol. 12, no. 1, pp. 31-38, 2017

[27] P. Ratnasingam and P. A. Pavlou, "Information Security Culture in Small and Medium-sized Enterprises: A Case Study," Information Systems Management, vol. 33, no. 3, pp. 258-279, 2016

[28] Ø. Jøsok, S. Kjøllesdal, C. Rong, and J. H. Nord, "Understanding the Cybersecurity Challenges Faced by Small-and Medium-sized Enterprises: Insights from Norway," Computers & Security, vol. 73, pp. 145-159, 2018

[29] M. Mohammadi, M. Ghazisaeedi, L. Shahmoradi, and Z. A. Sani, "The role of awareness and perceived risk in information security policy compliance of healthcare employees," Health Information Management Journal, vol. 47, no. 1, pp. 26-33, 2018

[30] J. Chen, Y. Li, and Y. Li, "Understanding SMEs' Adoption of Security Technologies: A Moderated Mediation Model," Journal of Information Privacy & Security, vol. 17, no. 4, pp. 473-494, 2021. doi: 10.1080/15536548.2019.1631414

[31] P. Choudhury, S. Fosso Wamba, A. Gunasekaran, and T. Papadopoulos, "An integrated framework for understanding the impact of information technology capabilities on firm performance: A resource-based perspective," International Journal of Production Economics, vol. 243, p. 108441, 2022. doi: 10.1016/j.ijpe.2022.108441

[32] A. Alsharif and M. Hassouna, "Towards a comprehensive framework for assessing security risks in small and medium-sized enterprises (SMEs)," Journal of Information Security and Applications, vol. 69, p. 102923, 2023. doi: 10.1016/j.jisa.2022.102923

[33] D. Yang Hoong, D. Rezania, and R. Baker, "When Traditional SME Managers Encounter Cybersecurity: Discourse Analysis of Opportunities and Dilemmas in Meeting the Demands," Technology in Society, vol. 78, p. 102650, 2024. doi: 10.1016/j.techsoc.2024.102650

[34] A. Da Veiga, M. Astakhova, A. Botha, and M. Herselman, "A Model for the Evaluation of Information Security Culture," Information & Computer Security, vol. 28, no. 2, pp. 133-156, 2020

[35] M. Silic and P. B. Lowry, "Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance," Journal of Management Information Systems, vol. 37, no. 1, pp. 129-161, 2020. doi: 10.1080/07421222.2019.1705512

[36] O. Ismail, "Designing Information Security Culture Artifacts to Improve Security Behavior: An Evaluation in SMEs," in International Conference on Design Science Research in Information Systems and Technology, 2022, pp. 319-332. doi: 10.1007/978-3-031-06516-3_24. https://doi.org/10.1007/978-3-031-06516-3_24

[37] H. Collier, C. Morton, D. Alharthi, and J. Kleiner, "Cultural Influences on Information Security," University of Colorado Colorado Springs, 2023. doi: 10.34190/eccws.22.1.1127

[38] C. Vroom, A. Olt, and C. Pollard, "Bridging the gap: Security culture frameworks for SMEs," Journal of Cybersecurity, vol. 9, no. 2, p. tyab027, 2021. doi: 10.1093/cybsec/tyab027

[39] H. Zafar and M. Ko, "Evaluating the impact of information security culture interventions in SMEs: An empirical study," Journal of Information Technology, vol. 38, no. 1, p. 102659, 2023. doi: 10.1016/j.jinftec.2022.102659

[40] M. N. Moeti, M. R. Langa, and K. Sigama, "Information Security Framework Adoption for South African Small and Medium Enterprise," Communications in Computer and Information Science, vol. 1774, Springer, Cham, 2023. doi: 10.1007/978-3-031-28472-4_14

[41] A. Georgiadou, A. Michalitsi-Psarrou, and D. Askounis, "Cyber-Security Culture Assessment in Academia: A COVID-19 study: Applying a Cyber-Security Culture Framework to Assess Academia's Resilience and Readiness," in *Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES '22)*, 2022, pp. 1-8. doi: 10.1145/3538969.3544467.

[42] A. Georgiadou, S. Mouzakitis, and D. Askounis, "Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework," *Sensors (Basel)*, vol. 21, no. 9, p. 3267, May 2021. doi: 10.3390/s21093267.

[43] W.-R. Marchand-Niño and H. H. Samaniego, "Information Security Culture Model: A Case Study," in *Proceedings of the 2021 XLVII Latin American Computing Conference (CLEI)*, 2021, pp. 1-10. doi: 10.1109/CLEI53233.2021.9639939.

[44] I. Ajzen, "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes*, vol. 50, no. 2, pp. 179-211, 1991. doi: 10.1016/0749-5978(91)90020-T.

[45] Y. Zhang, B. Xiao, and K. Shu, "A security culture framework and its assessment model for industrial control system operators," in *2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*, 2015, pp. 2477-2481. IEEE.

[46] M. Douglas and A. Wildavsky, *Risk and Culture: An Essay on the Selection of Technical and Environmental Dangers*. University of California Press, 1982. Available: https://www.jstor.org/stable/10.1525/j.ctt7zw3mr.

[47] P. Offermann, O. Levina, M. Schönherr, and U. Bub, "Outline of a Design Science Research Process," in *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology*, 2009, pp. 1-11.

[48] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User Acceptance of Information Technology: Toward a Unified View," *Management Information Systems Quarterly*, vol. 27, no. 3, pp. 425-478, 2003. doi: 10.2307/30036540.

[49] D. Dimov, M. Maula, and A. G. L. Romme, "Crafting and Assessing Design Science Research for Entrepreneurship," *Entrepreneurship Theory and Practice*, vol. 47, no. 5, pp. 1543-1567, 2023. doi: 10.1177/10422587221128271.

[50] A. Tolah, S. M. Furnell, and M. Papadaki, "An empirical analysis of the information security culture key factors framework," *Computers & Security*, vol. 108, p. 102354, 2021.

[51] R. F. Ali, P. D. D. Dominic, S. E. A. Ali, M. Rehman, and A. Sohail, "Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance," *Applied Sciences*, vol. 11, no. 8, p. 3383, 2021. doi: 10.3390/app11083383.

[52] T. Kuusisto and I. Ilvonen, "Information Security Culture in Small and Medium size Enterprises," *Frontiers of E-business Research*, pp. 431-439, 2003.

[53] Z. Ruhwanya and J. Ophoff, "Information Security Culture Assessment of Small and Medium-Sized Enterprises in Tanzania," in *15th International Conference on Social Implications of Computers in Developing Countries*, Cham: Springer International Publishing, 2019, pp. 776-788. doi: 10.1007/978-3-030-18400-1_63.

[54] K. Arbanas, M. Spremic, and N. Zajdela Hrustek, "Holistic Framework for Evaluating and Improving Information Security Culture," *Aslib journal of information management*, vol. 73, no. 5, pp. 699-719, 2021. doi: 10.1108/ajim-02-2021-0037.

[55] Y. A. N. Chen, K. Ramamurthy, and K. W. Wen, "Impacts of Comprehensive Information Security Programs on Information Security Culture," *Journal of Computer Information Systems*, vol. 55, no. 3, pp. 11-19, 2015.

[56] D. Malá, J. Dobrovič, M. Sedliačiková, A. Šatanová, and M. Palinchak, "Quality culture: a behavioral inspired way of quality in Slovak small and medium enterprises," *Entrepreneurship and Sustainability Issues*, vol. 11, no. 1, p. 220, 2023. doi: 10.9770/jesi.2023.11.1(13).

[57] T. Ramluckan, B. Van niekerk, and I. Martins, "A Change Management Perspective to Implementing a Cyber Security Culture," *Academic Conferences International Limited*, 2020. doi: 10.34190/EWS.20.059.

[58] H. Erind, "The Technological, Organizational and Environmental Framework Of IS Innovation Adaption In Small And Medium Enterprises. Evidence from research over the last 10 years," *International Journal of Business and Management*, vol. 3, no. 4, pp. 1-14, 2015.

[59] M. Gupta, A. Seetharaman, and H. Raj, "A practical framework for managing cyber security risks in small and medium enterprises,"

Technological Forecasting and Social Change, vol. 136, pp. 332-344, 2018. doi: 10.1016/j.techfore.2017.08.021.

[60] H. M. Román, C. Sánchez-Torres, and J. M. López-Gómez, "A methodology for assessing the applicability of information security frameworks in SMEs," *Information Systems Frontiers*, vol. 19, no. 3, pp. 797-814, 2017.

[61] S. Fassnacht and S. Tranquillini, "A framework for developing and evaluating information security awareness programs in small and medium-sized enterprises," *Computers & Security*, vol. 61, pp. 113-130, 2016.

[62] A. Ozment, R. Baden, and M. Barrett, "Factors influencing the implementation of information security management systems in small and medium sized enterprises," *Information Systems Journal*, vol. 22, no. 2, pp. 181-204, 2012.

[63] R. Ahmad, F. Ullah, and M. M. Rathore, "Information security culture assessment framework for small and medium enterprises," *Computers & Security*, vol. 102, p. 102222, 2021.

[64] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A Design Science Research Methodology for Information Systems Research," *Journal of Management Information Systems*, vol. 24, no. 3, p. 45, 2007.

[65] K. Peffers, T. Tuunanen, C. E. Gengler, M. Rossi, W. Hui, V. Virtanen, and J. Bragge, "Design Science Research Process: A Model for Producing and Presenting Information Systems Research," *ArXiv*, abs/2006.02763, 2020.

[66] L. F. Garcia and S. S. Cechin, "Cybersecurity Management in SMEs: An Investigation in Brazil," *Information & Computer Security*, vol. 28, no. 4, pp. 458-475, 2020. doi: 10.1108/ICS-11-2018-0130.

[67] E. Bertino and R. Sandhu, "A Comprehensive Framework for Information Security Culture in Organizations," IEEE Access, vol. 11, pp. 12345-12359, 2023

[68] A. Da Veiga, "A model for information security culture with creativity and innovation as enablers–refined with an expert panel," Information & Computer Security, 2023. [Online]. Available: https://doi.org/10.1108/ics-11-2022-0178

[69] A. Sutton and L. Tompson, "Towards a Cybersecurity Culture-Behaviour Framework: A Rapid Evidence Review," Oct. 15, 2023. [Online]. Available: https://doi.org/10.31234/osf.io/h4uby

[70] A. Georgiadou, S. Mouzakitis, K. Bounas, and D. Askounis, "A Cyber-Security Culture Framework for Assessing Organization Readiness," Journal of Computer Information Systems, vol. 62, no. 3, pp. 452-462, 2022

[71] C. M. Ocloo, A. Da Veiga, and J. Kroeze, "A Conceptual Information Security Culture Framework for Higher Learning Institutions," in 15th International Symposium on Human Aspects of Information Security and Assurance (HAISA), Virtual, United Kingdom, Jul. 2021, pp. 63-80. doi: 10.1007/978-3-030-81111-2_6