Journal of Information Systems and Informatics
Vol. 7, No. 1, March 2025 e-ISSN: 2656-4882 p-ISSN: 2656-5935
DOI: 10.51519/journalisi.v7i1.927 Published By DRPM-UBD

Strategic Framework for Cybersecurity Policy Compliance in Namibian Organizations

Iyaloo N. Waiganjo[1], Jude Osakwe[2], Ambrose Azeta[3]

[1,2]Department of Informatics, Namibia University of Science and Technology (NUST), Windhoek, Namibia
[3]Department of Software Engineering, Namibia University of Science and Technology (NUST), Windhoek, Namibia
Email: [1] in11waiganjo@gmail.com, [2] josakwe@nust.na, [3] aazeta@nust.na

Abstract

The Internet and its transformative technologies have become essential to both emerging and established businesses. While organisations benefit from connectivity, they are also increasingly vulnerable to cyber-attacks, underscoring the need for robust monitoring systems and comprehensive cybersecurity policies. In Namibia, many organisations have cybersecurity policies, yet employees are often unaware of existence of such policies. This study aimed to examine the complexities of cybersecurity policies within Namibian organisations and provide a tailored roadmap for developing, implementing, and ensuring compliance with these policies to suit the unique landscape of Namibian businesses. Using a qualitative approach guided by design science research, data was collected from 21 participants, including Information Technology (IT) and security managers as well as employees from five organisations across various sectors in the country. The findings indicated that Namibian organisations are commitment to cybersecurity through comprehensive policies aligned with international standards. However, organisations face impediments that underscore the need for targeted strategies to overcome barriers to policy enforcement. From these finding a framework was designed with strategies and action plans and evaluated by industry experts. The CSPIC framework was considered Good (rating 2) in most areas by the experts. Gaps in existing frameworks such as usability, adoptability, and budget prioritization were addressed by the proposed CSPIC framework. The Cybersecurity Policy Implementation and Compliance (CSPIC) framework's uniqueness lies in its local adaptability, actionable strategies, and emphasis on leadership and employee engagement.

Keywords: Cybersecurity Policy, Compliance, Organisational Framework, Namibia

1. INTRODUCTION

The relationship between businesses and the Internet has become more pronounced, with organisations strategically tethering their business models and structural frameworks to the vast expanse of digital connectivity [1]. The Fourth Industrial Revolution (4IR), characterised by the Internet of Things (IoT), further amplifies this interconnection, granting organisational business models with unknown capabilities through the integration of objects and people. Notably, the

Internet, with its transformative technologies, has assumed a pivotal role as the cornerstone for both nascent and established business ventures [2]. To safeguard an organisation's internet space, information, and communication technologies, many organisations are investing substantially in cybersecurity these days [3]. The inherent vulnerability of the Internet surfaced the way for an alarming surge in cybercrime, transforming it into a universal and profitable business enterprise [4]. Cyber threat actors in 2023 are increasingly adopting sophisticated attack strategies that have shown a notable success rate and return on investment (ROI) in the past, largely pushed by the recent advancements in Artificial Intelligence (AI), as highlighted by [5]. While organisations reaped the benefits of connectivity, they simultaneously opened themselves to cyber-attacks, necessitating the development of robust monitoring systems through the establishment of comprehensive cybersecurity policies. Policies documents which are mechanisms developed by an organisation which consists in the implementation of security controls [3].

These policies define acceptable use, access controls, incident response procedures, and encryption protocols among others [6]. They establish a framework for employees to adhere to security measures and enforce compliance with cybersecurity standards. However, in this well-intentioned quest for cyber resilience, organisations faced an enduring challenge of employee compliance. Despite the careful crafting of cybersecurity policies, employees often exhibited carelessness and indifference, overlooking, or underestimating the gravity of these protocols [7,8]. Recognising that employees constitute the weakest link in the cybersecurity chain, organisations found themselves grappling with the potential consequences of non-compliance. The actions of employees, particularly violations of security policies and regulations, could render the organisation susceptible to cyber threats and attacks [9]. In the absence of a comprehensive policy implementation plan coupled with harsh employees' adherence, these policies risked relegation to the status of inconsequential artifacts within the organisational framework [10].

[11] stressed that when a business organisation is planning to implement cybersecurity strategies, one of the first things to do is to formulate a cybersecurity policy that will give guidance on the best practices and outline what employees should or shouldn't do. Though some studies [11,12] pointed out that many organisations in Namibia have cybersecurity policies, others [13; 14] pointed out that Namibia organisations lack best practices to combat cyber-attacks. This could be due to a lack of a security framework within which existing security policy should be implemented in Namibia. Furthermore, the study of [5] is in consonance with this, as the researcher indicated that policy without an implementation process may not necessarily lead to expected results. In addition, the study by [15] that assessed the culture of information security among the

employees in a selected organisation found that organisations have security policies in place; however, their employees were not aware of them. The probable reason for the employees' unawareness, was because of the non-involvement of top managers in the formulation and the implementation of the policy. Considering the non-involvement of top management, enforcement and compliance to the policy could be challenging and hence exposes the organisations to higher Cybersecurity risk. Thus, it is in the quest to fill this gap that this study's objective is to explore cybersecurity policy implementation, focusing on the role of top management and policymakers as well as employee's compliance with cybersecurity policies based on their actions and motives, and will develop a Cybersecurity framework for Cybersecurity policy implementation.

It is against this background that this study embarks on critical exploration. The aim is to not only dissect the complex dynamics of cybersecurity policies but, more crucially, to furnish a comprehensive roadmap tailored for the creation and implementation of cybersecurity policies and compliances specifically adjusted for the distinctive landscape of business organisations in Namibia. The main objective of this study was to provide a strategic framework for cybersecurity policy compliance in Namibian organizations. The rest of this manuscript is arranged as follows: Section 2 contains research methods, and the guidelines for the development of CSPIC framework. Section 3 enumerates the results and analysis of the study, as well as the description of the CSPIC framework. Section 5 discussed the research results, while section 6 concludes the article.

2. METHODS

The study used a qualitative research approach to examine participants' perceptions of cybersecurity policymaking and compliance within Namibian organisations. Qualitative methods were chosen for their ability to foster deep understanding and collaboration between researchers and participants. The study aimed to create a framework for improving cybersecurity policy implementation and compliance, guided by Design Science Research (DSR) principles, which involve creating and evaluating artifacts to bridge problems and solutions. The DSR framework was based on the "Relevance and Rigour" values from [16], ensuring the developed framework aligns with employees' needs for cybersecurity compliance. For the Cybersecurity Policy Implementation and Compliance (CS-PIC) framework to meet values for DSR framework, the following guidelines was followed as detailed in Table 1.

Table 1. The DSR Guidelines for the CSPIC Framework

DSR Guideline (Van de Merwe, Smuts & Gerber, 2020)	The Study's activities
Guideline 1: Research in design science	CSPIC Framework

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

DSR Guideline (Van de Merwe, Smuts & Gerber, 2020)		The Study's activities
Design as an Artefact	needs to result in a workable artifact, such as a construct, model, technique, or instantiation.	developed
Guideline 2: Problem Relevance	The goal of design science research is to create environmentally conscious answers to significant and pertinent business issues.	Review and analyse relevant literature and published the findings.
Guideline 3: Design Evaluation	A design artefact's quality, effectiveness, and utility must be thoroughly proven through competent evaluation techniques.	Analytical and simulation by cybersecurity policy marks experts.
Guideline 4: Research Contributions	Clear and verifiable contributions to the design artefact, design foundations, and/or design methodologies are necessary for effective design science research.	A CSPIC framework guide will be published, and thesis document will be published.
Guideline 5: Research Rigour	Applying exacting techniques to the creation and assessment of the design artifact is essential to design science research.	Feedback report from experts
Guideline 6: Design as a Search Process	Finding an effective artifact requires making use of all available tools to accomplish goals and adhere to legal requirements in the problematic environment.	Organisations involved in the study and a select few other organisations not involved in the study will receive access to the CSPIC Framework guide.
Guideline 7: Communication of Research	Effective communication of design science research is necessary to audiences with a focus on management and technology.	An oral presentation of CSPIC framework

Participants included employees and managers in IT and information security (IS) from registered organizations in Windhoek, identified through purposive and convenience sampling. Data was gathered from organizations in diverse sectors like education, finance, telecommunications, courier services, and government,

selecting individuals with policy formulation or IT governance experience and employees involved in daily cybersecurity compliance. The study involved 21 participants across five organisations. The reason for using 21 participants was because only expert opinions from cybersecurity professionals were needed to justify the authenticity of the information gathered from the respondents. Data was collected using semi-structured interviews and focus groups, and thematic analysis was applied to organize and interpret findings, following [17] for analyzing and reporting themes within the data.

3. RESULTS AND DISCUSSION

3.1 Background information of the participants

[18], highlighted that the world has not enough specialist in information security is necessary educational qualifications and experience. However, based on the findings, Managers in Organisations A, B, C, and E have significant qualifications related to IT governance and cybersecurity. These include ISO certifications, master's degrees, and specialized courses, indicating a high level of expertise. However, Organisation D's manager is relatively new to the position but possesses relevant certifications and has been involved in cybersecurity policy implementation. On the other hand, most Organisations (A, B, D, and E) have managers with direct experience in cybersecurity policy implementation. While Organisation C has been focused more on IT governance policy rather than direct cybersecurity policy implementation for now. The findings of this study agree with [19] when he said that an organisation needs to have an information security specialist who must have training and skills to implement security controls to protect an Organisation from cyber threats to mitigate these exposure risks. As indicated by the findings, many IT managers' roles are Information security managers, cybersecurity analysts and even if that was not the role, they have qualifications related to cyber security of information security.

The study's participants included qualified specialists in cybersecurity policy implementation who provided the necessary responses to the interview questions. This indicates that the study successfully engaged the appropriate experts, who offered valuable insights into the research questions. According to [8], qualitative research participants are chosen specifically to best inform the research questions, thereby enhancing the understanding and quality of the phenomenon under investigation. By selecting participants based on their expertise and relevance to the study, the research ensures that the data collected is both meaningful and comprehensive. The IT managers contributed significantly to the depth and reliability of the findings, as the insights from these specialists are directly applicable to the research objectives.

Across all Organisations, employees in various roles (procurement officers, data officers, financial accountants, levy collectors, help desk administrators, and system analysts) are involved in handling sensitive data. Moreover, Employees have varying lengths of service, from a few months to several decades, highlighting the need for ongoing training and updates to cybersecurity practices to accommodate both new hires and long-term staff.

3.2. Analysis on the prevailing IT governance practices towards cybersecurity

The prevailing IT governance practices across the Organisations reveal a multifaceted approach to managing and securing IT infrastructure, characterized by distinct themes. These themes provide insight into how Organisations implement, enforce, and continually improve their cybersecurity measures.

1) Policy Development and Framework Alignment

A study that was conducted by [20] concludes that having technological solutions for cybersecurity is not as crucial as establishing a set of information security policies and procedures. The findings of this study indicate that the development and review of cybersecurity policies are crucial in the face of increasing cyber-attacks. Organisation A Are in their third phase of implementing their cybersecurity and has a comprehensive Information Security policy spanning 130 pages, covering multiple areas. Regular reviews aligned with ISO 27001 standards and annual assessments ensure policies meet evolving security needs. Organisation B reviews its policies every three years, with urgent updates for emerging threats. Separate policies for IT security, cybersecurity training, incident response, data privacy, and information access avoid unwieldy documentation. Organisation C is in the process of developing a cybersecurity policy using the COBIT 5 2019 framework, and a recent penetration test highlighted vulnerability, guiding the development of new policies. Organisation D reviews policies every two years, adjusting for new threats. Their policies align with multiple frameworks (NIST, PCI DSS, King IV, NamCode) to ensure comprehensive coverage and responsiveness to emerging threats. Organisation E was involved in drafting a National Cybersecurity Strategy and is currently drafting its Organisational strategy, incorporating elements from the national strategy. They conduct quarterly audits to assess compliance, and policies are treated as living documents, regularly updated to adapt to new challenges.

2) Inclusive and Continuous Training

Study by [21] underscores the significance of security awareness training as an integral component in safeguarding companies against evolving and detrimental

cybersecurity threats. These findings highlight the need for a comprehensive and adaptable approach to cybersecurity training that caters to the diverse needs of trainees and keeps pace with the rapidly changing cyber landscape. For instance, Organisation A conducts regular weekly training sessions involving questionnaires and assessments to ensure employees remain aware of security protocols. Attendance is monitored, and non-compliance is addressed by supervisors. Organisation B opts for quarterly training sessions, including phishing simulations and personalized follow-ups, effectively enhancing awareness and comprehension. Immediate training on data protection and information access policies reinforces policy understanding. Organisation D organizes pre-implementation training sessions for new policies to help employees understand and comply. Regular meetings and the distribution of cybersecurity booklets, along with weekly email updates, keep staff informed and vigilant. Organisation E continuously holds cybersecurity awareness sessions in collaboration with MICT to educate employees and foster a cybersecurity culture. Assessments follow these sessions to gauge understanding and effectiveness.

3) Effective Communication

According to [19], trustworthy and effective communication of cybersecurity risks is particularly important, given the human element in security. This study demonstrated that effective communication of cybersecurity risks is crucial in building a cybersecurity culture and managing crisis events. Awareness and adherence to information security policies are key to protecting against cyber threats. Organisation A emphasizes continuous communication through emails, advisories, and weekly security checks to ensure employees are reminded of existing threats and countermeasures. This fosters a culture of vigilance and adherence to security protocols. Organisation B maintains a continuous feedback mechanism from regular penetration testing and phishing simulations, keeping staff informed and policies updated. Their communication is effectively stressed by leadership, which helps in successful policy implementation.

4) Technical Controls and Monitoring

Organisations deploy sophisticated tools and technologies for real-time monitoring of network activities, detecting anomalies, and identifying potential security breaches [22]. Security controls and measures are developed and used to guard data and information systems of the Organisation [23]. This study's findings have demonstrated the importance of technical controls and monitoring in cybersecurity. Most Organisations articulated different controls and monitoring techniques. For instance, Organisation A conducts weekly security checks to monitor unauthorized activities, with email inquiries sent for clarification. Policies mandate password changes every 30 days, and access to

certain websites is restricted to mitigate risks. Organisation B performs penetration testing and phishing simulations to measure staff response, using the data to refine policies. Regular feedback mechanisms and continuous updates maintain policy effectiveness. Organisation D includes frequent password changes and restrictions on software installation and website access in their policies. They also conduct regular audits and updates to ensure compliance and promptly address new threats. Organisation E implements security measures such as restrictions on website access and the prohibition of public Wi-Fi use for work emails. The findings highlight the importance of a multi-faceted approach to technical controls and monitoring in cybersecurity, encompassing proactive measures, continuous improvement, compliance enforcement, and risk mitigation strategies. By implementing a combination of these strategies tailored to their specific Organisational needs and risk profiles, Organisations can effectively bolster their defenses against cyber threats and safeguard their assets from potential breaches or unauthorized access [23].

5) Stakeholder Collaboration

A strategic dimension to successful cybersecurity policy implementation involves collaboration with stakeholders in the process [20]. The findings collectively underscore the critical role of collaboration and integration in cybersecurity, both at the international and Organisational levels. Organisation E works closely with other ministries on policy formulation and implementation. Regular internal reviews and assessments ensure policies align with national cybersecurity standards for the government. Organisation B collaborates with business strategy and risk management departments to ensure policies are effective and aligned with Organisational goals. Leadership involvement is crucial for policy enforcement and communication. Organisation A emphasizes inclusive participation from all staff members in policy formulation, ensuring insights from diverse perspectives are considered and fostering a culture of collaboration.

According to [20], stakeholders should not be passive recipients of policy; instead, they should be actively engaged throughout the implementation journey. The findings indicate that effective collaboration is an essential pillar of cybersecurity governance. By engaging with stakeholders both within and outside the Organisation, integrating established frameworks, aligning with Organisational goals, and fostering a culture of inclusivity, Organisations can enhance their resilience against cyber threats and effectively mitigate risks. The prevailing IT governance practices towards cybersecurity in Namibian Organisations reveal a comprehensive and multi-faceted approach that includes continuous training, robust policy development, effective communication, advanced technical controls, and strong stakeholder collaboration. Organisations emphasize regular and adaptive security awareness training, systematic policy

development and review, and proactive communication to foster a culture of vigilance. Sophisticated technical controls and real-time monitoring are employed to detect and mitigate threats, while active collaboration with internal and external stakeholders ensures alignment with Organisational goals and enhances resilience. By integrating these elements, Namibian Organisations have shown a significantly strength in their cybersecurity posture against evolving threats.

3.3. Analysis on the impediments to cybersecurity policy implementation in organisations

The impediments to cybersecurity policy implementation vary across Organisations but commonly include challenges related to compliance, training, budget constraints, communication. Which are categorized into two factors, Technological and Human factors. Human and technological factors play a critical role in cybersecurity challenges, particularly in the context of social engineering. Organisation E emphasized the importance of continuous awareness and training to create a strong cybersecurity culture. Organisation A highlighted the proactive approach of their security team, including regular training sessions and updates, which helped manage the constant stream of security tasks. However, the demanding nature of these tasks and the pressure to comply with guidelines remained significant challenges for employees. Differences between technology and human factors are:

1) Technological Factors

Technological factors often complicate cybersecurity policy adherence due to the operational burden they impose on employees. For instance, Organisation A's employees faced challenges with frequent security updates and notifications, which distracted them from their core tasks. These findings align with studies that highlight the impact of excessive system notifications on employee productivity and focus [24]. Additionally, Organisation D's struggle with managing frequent password changes, leading to memory issues and reduced productivity, reflects broader research on password management challenges in the workplace. According to [24], such frequent updates, although essential for security, often frustrate employees, contributing to poor adherence. The technological and human factors as the main influence of cybersecurity policy adherence, as outlined in the analysis, differ in several keyways.

2) Human Factors

Human factors, on the other hand, primarily concern behavioral and cognitive responses to cybersecurity policies. Organisation D’s resistance to policy compliance, especially among older employees due to cultural resistance and

ignorance, mirrors findings in the literature where human behavior is a key impediment to cybersecurity [3]. Moreover, Organisation C's lack of comprehensive training left employees unprepared for cybersecurity challenges, a common issue noted by [25]. Social engineering attacks, which exploit human vulnerabilities rather than technical weaknesses, emphasize the significance of human factors [26]. Human factors, therefore, necessitate a focus on continuous education, awareness, and training to improve adherence.

The finding shows that the implementation of cybersecurity policies faces several impediments across Organisations, including a lack of executive support, compliance and adherence issues, insufficient training and awareness, budget constraints, poor communication, and human factors. Addressing these challenges requires a multifaceted approach, involving strong leadership, comprehensive and continuous training programs, adequate resource allocation, and transparent communication. Building a culture of cybersecurity within Organisations is essential for mitigating these impediments and ensuring robust protection against cyber threats.

3.4. Analysis of the Strategies Employed by IT Leaders when implementing cybersecurity

Based on the findings from Organisations A, B, C, D, and E, IT leaders employ a variety of strategies to enforce and ensure adherence to cybersecurity policies. These themes encompass approaches and strategies that address various facets of cybersecurity, including awareness, communication, resource allocation, and collaboration.

1) Integrated and Continuous Communication

Effective cybersecurity policies are embedded within digital systems, ensuring that employees receive constant reminders and updates about security protocols. This approach helps maintain high levels of awareness and compliance. Organisation B said that “we encourage open communication channels for continuous feedback and clarification to ensure clear understanding of policies”. Participants from Organisation A highlighted the importance of these reminders in keeping everyone informed and vigilant, although some found the frequency of notifications overwhelming. As said by Orgnisations A managers that, “our work emails and devices feature regular reminders about threats, mitigations, and policy compliance. And organisation B send awareness resources through email communications. These reminders keep everyone informed about security protocols." Consistent and integrated communication is vital for maintaining cybersecurity awareness. Organisation D also has weekly emails with cybersecurity tips and plans for phishing simulations. According to [10], regular

communication and reminders about security protocols significantly reduce the likelihood of human errors, which are often the weakest link in cybersecurity defenses. Moreover, [27] emphasizes that embedding cybersecurity policies into digital workflows ensures that security becomes a part of daily routines, thereby enhancing compliance and vigilance among employees.

2) Resource Allocation and Budget Management

Despite budget constraints, Organisations find innovative ways to allocate resources towards cybersecurity training and awareness. Participants from Organisation C noted the value of external training despite financial limitations, and Organisation B emphasized the effectiveness of diverse educational resources. The variety of educational materials catered to different learning styles, enhancing overall comprehension and compliance. Budget constraints are a common impediment to effective cybersecurity policy implementation. However, as [28] points out, innovative resource allocation, such as leveraging external training programs and utilizing diverse educational materials, can mitigate these limitations.

3) Collaboration and Leadership Involvement

Leadership plays a crucial role in the successful implementation of cybersecurity policies. By endorsing and collaborating with stakeholders and external entities, leaders reinforce the importance of cybersecurity and drive collective efforts towards robust defense mechanisms. Participants from Organisation B and E underscored the importance of leadership involvement and inter-ministerial collaboration, which set strong examples and motivated employees. According to Organisation B leadership endorsement is crucial. Collaborating with stakeholders and sister companies has been vital for effective cybersecurity implementation and when our leaders actively participate in cybersecurity initiatives, it sets a strong example and motivates the entire team to prioritize security."

4) Awareness and Training Programs

Continuous training and awareness programs are vital in fostering a culture of cybersecurity. Regular sessions, practical assessments, and simulations ensure that employees remain vigilant and are equipped to handle cyber threats effectively. Participants from Organisation A, D and E shared their positive experiences with ongoing training and assessment initiatives, noting that these programs were engaging and provided real-world applications of cybersecurity practices. As highlighted by Organisation D managers that, “we conduct continuous training and awareness programs. It's crucial to keep everyone in the Organisation aware

of the latest threats and best practices." And the despondences from Organisation E "Weekly awareness sessions and assessments help us stay prepared and gauge our understanding of cybersecurity threats." Organisation A said, "We strongly advocate for Organisations to prioritize cybersecurity awareness as a critical security imperative".

5) Comprehensive and Multifaceted Approaches

A holistic approach that combines technical measures with human behavior policies provides a robust defense against cyber threats. Addressing both technical and cultural aspects ensures comprehensive protection. Organisation A participants noted the benefits of integrating technical and behavioral policies, while Organisation D participants emphasized the importance of addressing both work and home environments. Involving HR helped drive cultural change, making cybersecurity a shared responsibility.

6) Regular Auditing and Policy Updates

Regular auditing and assessments help Organisations refine and update their cybersecurity policies. Feedback mechanisms and continuous evaluations ensure that policies adapt to new threats and remain effective over time. Participants from Organisation B and E highlighted the critical role of regular audits and open communication in maintaining effective cybersecurity policies. Feedback from employees was crucial in refining policies to make them more practical and user-friendly. Participant Response from Organisation B "Regular auditing and assessments are essential for keeping our policies effective and up to date with the latest threats." An additional participant response Organisation B said that, "these audits help us identify weak points and improve our security measures continuously." While, Organisation E said that "Continuous audits and policy reviews help us adjust and improve our cybersecurity measures." Additional Organisation E "Regular assessments ensure that our cybersecurity practices evolve with the changing threat landscape."

The findings illustrate a multifaceted approach to cybersecurity policy implementation. Successful strategies include integrated communication, resource allocation despite budget constraints, strong leadership involvement, continuous awareness and training, comprehensive technical and behavioral policies, and regular auditing. These elements collectively contribute to creating a resilient cybersecurity posture within Organisations. The participant responses provide valuable insights into the practical application and effectiveness of these strategies in fostering a secure Organisational environment.

3.5. Cybersecurity Policy Implementation and Compliance (CSPIC) Framework Development

Based on the analysis, developing a comprehensive cybersecurity framework tailored for Namibian organisations involves addressing both cybersecurity policy implementation challenges and ensuring employee compliance. The framework integrates best practices from existing findings, consider the unique challenges and opportunities within the Namibian context, and leverage insights from the analysis of the five organisations and the literature. The framework has eight (8) strategies with very well-articulated action plans, the strategies are put together by an actor who is the cybersecurity personnel as illustrated in Figure 1. Using the Delphi technique, the study employed expert reviews to assess the usability, adoptability, effectiveness, relevance, and overall assessment of the CSPIC framework. The Delphi technique involves a process of sending a series of questions to experts in the industry to validate the framework [28].

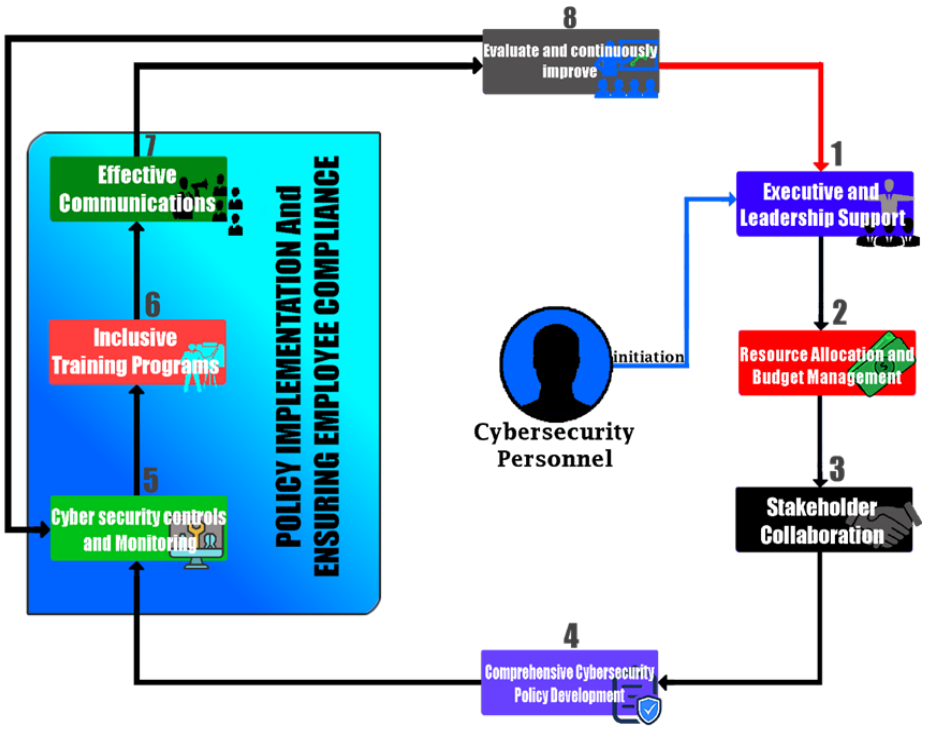

Figure 1. Cybersecurity Policy Implementation and Compliance (CSPIC) Framework

1) Cybersecurity Personnel: Ensuring Successful Framework Implementation

For any organisation aiming to implement successful cybersecurity policies and achieve employee compliance, having a dedicated executive responsible for information security is crucial. This individual, often referred to as a Chief Information Security Officer (CISO) or similar title, plays a pivotal role in overseeing and ensuring the successful implementation of the cybersecurity framework [19].

A dedicated cybersecurity executive is essential for the successful implementation of a comprehensive cybersecurity framework. With the right experience, qualifications, and strategic vision, this executive ensures that cybersecurity initiatives are effectively integrated into the Organisation's operations. Their role includes overseeing implementation and assigning tasks to ensure that all elements of the framework are accomplished. Define and monitor Key Performance Indicators (KPIs) such as time to detection, time to response, number of incidents, and compliance scores. The cybersecurity executive personnel are responsible for assuring that the following strategies are carried out.

2) CSPIC framework Strategies

A strategy in a framework is a systematic approach to guide decision-making and achieve organisational goals. Strategy is a multifaceted concept with roots in every organisation's planning context [29; 30]. It is generally defined as a high-level plan to achieve long-term goals under uncertainty [29] or a detailed plan for success in various situations [30]. [31] offers a more precise definition, describing strategy as the "smallest set of choices and decisions sufficient to guide all other choices and decisions. The framework outlines a major set of choices the cybersecurity executive person needs to carry out with in the major choices there are action actives outlined in detail. The action activities are referred to action plans.

3) Executive and Leadership Support Strategy

Secure commitment from top leadership. The strategy of securing commitment from top leadership is a pivotal component of ensuring effective cybersecurity policy implementation within organisations [24]. This strategy entails garnering support, engagement, and active involvement from senior executives, including CEOs, managing directors, and other top decision-makers.
Action plans:

a) Establishing Understanding and Awareness

b) Aligning Cybersecurity with Business Objectives
c) Integrate Cybersecurity into Governance Structures

4) Resource Allocation and Budget Management strategy

Integrating cybersecurity budgeting into strategic planning is essential to ensure that adequate resources are available for protection, monitoring, and response efforts. Organisations must allocate sufficient financial and human resources to maintain a strong cybersecurity posture, safeguarding critical assets and ensuring business continuity. Once management support is secured, resources can be appropriately allocated and approved [32]. Budgeting must be tailored to the organization's specific resources and needs, as a one-size-fits-all approach is ineffective. For multi-branch organisations, cybersecurity investments should account for factors such as the size of the information network, system interconnectivity, and the likelihood of threat propagation. In situations where budgets are constrained and vulnerabilities are high, protecting the headquarters often takes priority. Additionally, security information sharing across branches can enhance overall investment efficiency.
Action plans:

a) Develop a Detailed Cybersecurity Budget Proposal
b) Seek External Funding or Partnerships to Support Cybersecurity Initiatives
c) Leverage Third-Party Services

5) Stakeholder Collaboration Strategy

Stakeholder collaboration is crucial for effective cybersecurity strategies. [33] emphasize that despite diverse interests, stakeholders like National Cybersecurity Incident Response Team NCIRTs, security providers, and governments share fundamental security goals, necessitating cross-border cooperation. Foster collaboration with internal and external stakeholders. Collaboration with both internal and external stakeholders is essential for creating a robust and proactive cybersecurity environment. Engaging a wide range of perspectives and expertise enhances the organisation's ability to defend against cyber threats and ensures that policies and practices are comprehensive and effective.
Action Plans:

a) Collaborating with Government Agencies, Industry Bodies, and Other Organisations
b) Establish Internal Committees for Cybersecurity Policy Implementation
c) Engage Employees in Policy Formulation

6) Comprehensive Cybersecurity Policy Development Strategy

To safeguard organisational assets and ensure compliance, developing and maintaining robust cybersecurity policies is essential. With support from the executives and relevant information from the stakeholders, this strategy involves creating a comprehensive set of guidelines and procedures to protect against cybersecurity threats and ensure regulatory compliance. Organisations must be aware of applicable laws, regulations, and standards to create appropriate policies and controls [33]. To create effective policies, organisations should identify their audience, choose a framework, establish drafting and publishing processes, communicate and train employees, and monitor compliance [34]. By implementing comprehensive cybersecurity policies, organisations can mitigate risks, protect sensitive information, and avoid potential financial and reputational damage.

Action plans:

a) Leverage Established Internation Frameworks and standards
b) Tailor Policies for Specific Threats and Regulatory Requirements
c) Regular Review and Updates

7) Cyber Security Controls and Monitoring Strategy:

Effective technical controls and continuous monitoring are critical components of an organization's cybersecurity policies. By leveraging advanced technologies and methodologies, organisations can proactively detect, mitigate, and respond to threats, ensuring the security and integrity of their information systems as it has been articulated in the policy. Continuous monitoring is a critical component of cybersecurity strategies, providing real-time visibility into organizational assets, threats, vulnerabilities, and the effectiveness of security controls [36]. This approach represents a significant shift from periodic assessments to ongoing evaluation of vital security controls, enabling timely risk mitigation and informed decision-making. The implementation of continuous monitoring in high-performance computing environments presents unique challenges, requiring tailored solutions for complex systems [35].

Action plans:

a) Deploy Advanced Cybersecurity Tools: Both technical controls and physical controls must be implemented to ensure comprehensive cybersecurity protection.
b) Conduct Regular Security Assessments
c) Enforce Strict Access Controls
d) Control Internet Access and Network Use
e) Regular Updates and Patching

8) Inclusive Training Programs Strategy:

This strategy will shift employee's behaviour from mere having awareness to active participation in cybersecurity practices, ensuring that employees not only know the policies but also consistently apply safe behaviors in daily operations. Inclusive cybersecurity training programs are crucial for shifting employee behavior from mere awareness to active participation in security practices. Research suggests that successful programs should relate cybersecurity to employees' personal lives, reinforce guidelines, and minimize security fatigue [37]. Key attributes for driving behavior change include obtaining senior management support, treating awareness as a continuous process, cultivating cybersecurity as a norm, and using incentives and persuasive messaging.
Action Plans:

a) Conduct Regular, Mandatory Training Sessions for All Employees
b) Utilizing Diverse Training Methods
c) Tailor Training Content to Different Roles and Levels within the Organization
d) Partner with Local Educational Institutions and Cybersecurity Experts for Training
e) Implementing a Continuous Improvement Process
f) Analyze Training Outcomes and Update Training Programs

9) Effective Communication Strategy:

Effective communication is crucial for establishing a robust cybersecurity culture within organisations. Clear, understandable messaging that balances positive and negative elements is essential to engage employees and prevent passive behavior [41]. Organisations should integrate communication plans into their cybersecurity strategies, ensuring quick response during emergencies and system failures [38]. To effectively communicate cybersecurity risks, organisations should focus on information trust, risk communication, and security usability [40]. Cybersecurity awareness and education programs play a vital role in cultivating a cyber-resilient workforce. These programs employ various methodologies, including interactive workshops, simulated phishing exercises, and gamified learning platforms. Employee engagement and accountability are key factors in sustaining the efficacy of cybersecurity initiatives. Establishing clear and effective communication channels ensures that all employees are informed, engaged, and proactive in maintaining cybersecurity.
Action plans:

a) Cultivate a Cybersecurity Culture
b) Provide Support and Resources
c) Regular Communication
d) Utilize Multiple Communication Channels

e) Encourage Open Communication and Feedback

10) Evaluate and Continuously Improve Strategy:

The final strategy focuses on the evaluation and continuous improvement of all previously implemented cybersecurity strategies. This overarching strategy ensures that each of the first seven strategies is effectively executed and continuously enhanced to adapt to evolving threats and organisational needs.
Action Plans:

a) Schedule for Regular Review Meetings
b) Develop Detailed Evaluation Checklists
c) Ensure Senior Executive Involvement

By integrating the above ten strategies, coordinated by cybersecurity executive personnel, will empower organisations to implement cybersecurity policies effectively and foster employee compliance with policies and procedures. This approach builds a strong cybersecurity culture and ensures comprehensive protection across the organization.

3.6. Discussions

The CSPIC Framework offers a robust blueprint for addressing cybersecurity policy challenges and fostering compliance. Its emphasis on leadership support, stakeholder collaboration, training, and continuous improvement ensures adaptability and long-term success. By leveraging expert input and aligning strategies with Namibia's unique needs, the framework is positioned to significantly enhance organizational cybersecurity resilience. To demonstrate the uniqueness and adaptability of the CSPIC Framework, it is important to analyze how it aligns or diverges from other cybersecurity frameworks developed globally. Here's a comparative analysis as shown in Table 2.

Table 2: Comparisons of CSPIC Framework to global Frameworks and Standards

Frameworks/Standard	Key Features of Frameworks	Comparison to CSPIC Framework
United States (NIST Cybersecurity Framework)	Focus on five core functions: Identify, Protect, Detect, Respond, Recover. Offers a flexible, risk-based approach adaptable to different sectors [42].	CSPIC adopts a similar flexible approach, emphasizing continuous improvement and adaptability to threats. However, it places greater emphasis on leadership engagement and resource constraints, tailored to Namibia's unique

Frameworks/Standard	Key Features of Frameworks	Comparison to CSPIC Framework
		organizational challenges.
European Union (GDPR-aligned Frameworks)	Centered around compliance with data protection and privacy laws. Strong emphasis on stakeholder engagement and legal conformity [43].	CSPIC integrates stakeholder collaboration and compliance but extends beyond data privacy to address broader challenges such as budget constraints and inclusive training programs.
Africa (African Union Convention on Cybersecurity and Data Protection)	Focuses on harmonizing cybersecurity practices across member states. Highlights resource constraints and skill gaps [44].	CSPIC aligns well with African contexts by addressing resource allocation and emphasizing training. However, it introduces detailed action plans for each strategy, making it more actionable than high-level policy recommendations.
Asia-Pacific (APEC Cybersecurity Framework)	Emphasizes public-private partnerships and international collaboration. Stresses information sharing and capacity building [45].	CSPIC incorporates similar collaborative principles but is more specific in its localized strategies, such as focusing on stakeholder collaboration and leveraging partnerships for training and resources.
ISO/IEC 27000 Standards	Provides a systematic approach to information security management. Emphasizes leadership involvement, risk-based thinking, and continual improvement [46].	CSPIC aligns with ISO/IEC 27000 standards by integrating leadership-driven strategies, risk assessment, and continuous improvement. Additionally, CSPIC offers specific localized strategies, such as addressing stakeholder collaboration and adapting to Namibia's unique challenges, including resource constraints.

CSPIC Framework did not align and adapt the regional and international frameworks and standards, it has its own uniqueness as described here:

a) Local Adaptation: Tailored for Namibian organizations, addressing context-specific issues like budgetary constraints, resource limitations, and a lack of specialized personnel.
b) Leadership Emphasis: Stronger focus on securing leadership commitment compared to other frameworks, recognizing the critical role of top executives in resource allocation and policy enforcement.
c) Actionable Strategies: Detailed action plans under each strategy ensure practical implementation, contrasting with the broader guidance in some international frameworks.
d) Training and Behavior Change: While international frameworks discuss awareness, CSPIC prioritizes inclusive training to shift employee behavior from awareness to active participation.

The comparison of the CSPIC Framework with globally recognized cybersecurity frameworks, such as NIST, ISO/IEC 27000 standards, and regional frameworks like GDPR and the African Union Convention, highlights its uniqueness and adaptability to the Namibian context. While CSPIC aligns with international best practices by incorporating leadershipdriven strategies, stakeholder collaboration, risk-based approaches, and continuous improvement, it stands out by addressing Namibia-specific challenges, such as resource allocation, skill gaps, and organizational budget constraints.

The CSPIC Framework demonstrates its practicality through detailed, actionable strategies and localized implementation plans that make it more applicable to the realities of Namibian organizations compared to the high-level recommendations often found in other frameworks. Its alignment with international standards ensures global relevance, while its tailored approach makes it a robust and context-specific tool for strengthening cybersecurity policy implementation and compliance in Namibia.

4. CONCLUSION

This study highlights the urgent need for a comprehensive and context-specific approach to cybersecurity policy implementation and compliance within Namibian organisations. The development of the Cybersecurity Policy Implementation and Compliance (CSPIC) Framework marks a significant milestone in addressing the unique challenges that these organisations face in an increasingly complex digital landscape. By tailoring this framework to local conditions, the research contributes valuable insights into the specific vulnerabilities and needs of Namibian enterprises. The findings from the interviews and expert evaluations reveal that while many organisations have

established a foundational level of cybersecurity practices, there remains considerable potential for enhancement. The organisations involved in this study demonstrated a clear commitment to improving their cybersecurity posture; however, persistent barriers such as insufficient leadership support, inadequate training programs, and limited resource allocation continue to hinder effective policy implementation. The CSPIC framework aims to bridge these gaps by providing a structured approach that emphasizes the integration of technical controls with human-centric policies, fostering a culture of cybersecurity awareness and compliance among employees.

The CSPIC framework serves as a proactive initiative that not only addresses immediate cybersecurity concerns but also establishes a foundation for long-term resilience and adaptability in the face of evolving threats. By offering practical guidance tailored to the unique challenges faced by Namibian organisations, this framework has the potential to become a leading model for organizational cybersecurity.Moreover, the CSPIC Framework has significant practical applications across various sectors in Namibia, beyond its primary focus on organizational cybersecurity. In sectors such as education, healthcare, finance, and government, the framework can guide the development of tailored cybersecurity policies and practices to address sector-specific challenges.

To ensure the CSPIC Framework evolves alongside the rapidly changing cybersecurity landscape, future research should focus on expanding the framework to address risks associated with advanced persistent threats (APTs), artificial intelligence-driven attacks, and quantum computing. This can include proactive strategies for managing such threats. Future research should also include expanding the framework to include other critical sectors in Namibian economy such as healthcare, finance, agriculture, tourism and a lot more. Moreso, investigate how the framework can foster collaboration with regional and international cybersecurity initiatives to harmonize practices and share threat intelligence.

REFERENCES

[1] M. Lezzi, M. Lazoi, and A. Corallo, "Cybersecurity for Industry 4.0 in the current literature: A reference framework," *Comput. Ind.*, vol. 103, pp. 97–110, 2018.

[2] M. Kiskis, "Entrepreneurship in cyberspace: what do we know?" *Int. J. Entrepreneurial Behav. Res.*, vol. 17, no. 2, pp. 200–217, 2011.

[3] A. Mishra, Y. I. Alzoubi, A. Q. Gill, and M. J. Anwar, "Cybersecurity enterprises policies: A comparative study," *Sensors*, vol. 22, no. 2, p. 538, 2022.

[4] J. Ursillo and C. Arnold, "Cybersecurity is critical for all organisations – large and small," *Cyber Secur. Rev.*, vol. 1, no. 4, pp. 12–18, 2019.
[5] G. Grispos, "Cybersecurity: Practice," *Encycl. Secur. Emerg. Manag.*, pp. 1–6, 2019.
[6] N. S. Safa et al., "Information security conscious care behaviour formation in organisations," *Comput. Secur.*, vol. 53, pp. 65–78, 2015.
[7] L. Li et al., "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior," *Int. J. Inf. Manag.*, vol. 45, pp. 13–24, 2019.
[8] M. S. Jalali et al., "Why employees (still) click on phishing links: Investigation in hospitals," *J. Med. Internet Res.*, vol. 22, no. 1, p. e16775, 2020.
[9] R. A. Alias, "Information security policy compliance: Systematic literature review," *Procedia Comput. Sci.*, vol. 161, pp. 1216–1224, 2019.
[10] D. Tjirare and F. Bhunu Shava, "Developing security metrics to evaluate employee awareness: A case of a Ministry in Namibia," *Namibian J. Res. Sci. Technol.*, vol. 1, no. 1, pp. 11–18, 2018.
[11] P. T. Shambabi, S. Musarurwa, and F. Bhunu Shava, "Assessing organisational information security culture among workforce in universities: A case of Namibia," in *Proc. 2021 IST-Africa Conf.*, 2021, pp. 1–8.
[12] A. Van der Merwe, A. Gerber, and H. Smuts, "Guidelines for conducting design science research in information systems," in *Proc. Annu. Conf. South. Afr. Comput. Lect. Assoc.*, Cham, Switzerland: Springer, 2019, pp. 163–178.
[13] L. S. Nowell et al., "Thematic analysis: Striving to meet the trustworthiness criteria," *Int. J. Qual. Methods*, vol. 16, no. 1, p. 1609406917733847, 2017.
[14] M. Spruit, "Information security education based on job profiles and the e-CF," *High. Educ. Skills Work-Based Learn.*, vol. 12, no. 2, pp. 294–308, 2022.
[15] S. Cotton, "Experience and qualifications required for a Chief Information Security Officer: An e-Delphi study," Ph.D. dissertation, Univ. Phoenix, 2022.
[16] H. Aldawood and G. Skinner, "Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues," *Future Internet*, vol. 11, no. 3, p. 73, 2019, doi: 10.3390/fi11030073.
[17] R. Sabillon, J. J. Cano, and J. Serra-Ruiz, "Cybercrime and cybercriminals: A comprehensive study," *Int. J. Comput. Netw. Commun. Secur.*, vol. 4, no. 6, pp. 165–173, 2016.
[18] J. R. C. Nurse, "Cybersecurity risk communication: Understanding information trust and security usability," *IEEE Commun. Surv. Tutor.*, vol. 15, no. 4, pp. 1475–1490, 2013, doi: 10.1109/SURV.2013.013013.00142.

[19] I. Corradini, "Shaping cybersecurity awareness programs: Lessons from behavioral sciences," *Cyberpsychol. Behav. Soc. Netw.*, vol. 23, no. 5, pp. 333–341, 2020, doi: 10.1089/cyber.2019.0428.
[20] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, 2018.
[21] European Union, *General Data Protection Regulation (EU GDPR)*, 2016.
[22] African Union, *African Union Convention on Cybersecurity and Personal Data Protection*, 2014.
[23] Asia-Pacific Economic Cooperation, *APEC Framework for Securing the Digital Economy*, 2015.
[24] International Organization for Standardization, *ISO/IEC 27001:2022 Information Security Management Systems – Requirements*, 2022.
[25] M. Alqahtani and R. Braun, "Examining the impact of technical controls, accountability and monitoring towards cybersecurity compliance in e-government organisations," *J. Cyber Secur. Technol.*, vol. 5, no. 3, pp. 203–221, 2021.
[26] M. Alotaibi, S. Furnell, and N. Clarke, "Information security policies: A review of challenges and influencing factors," in *Proc. 11th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, 2016, pp. 352–358.
[27] S. Kumari, A. Thompson, and S. Tiwari, "6G-Enabled Internet of Things-Artificial Intelligence-Based Digital Twins: Cybersecurity and resilience," in *Emerg. Technol. Secur. Cloud Comput.*, IGI Global, 2024, pp. 363–394.
[28] M. F. Safitra, M. Lubis, and H. Fakhrurroja, "Counterattacking cyber threats: A framework for the future of cybersecurity," *Sustainability*, vol. 15, no. 18, p. 13369, 2023, doi: 10.3390/su151813369.
[29] M. Barad and M. Barad, "Definitions of strategies," in *Strategies and Techniques for Quality and Flexibility*, IGI Global, 2018, pp. 3–4.
[30] D. Dalcher, "Taking responsibility for our actions: The return of stewardship," *PM World J.*, vol. VIII, no. VII, 2019.
[31] E. Van den Steen, "A formal theory of strategy," *Manage. Sci.*, vol. 63, no. 8, pp. 2616–2636, 2017.
[32] T. Fagade, K. Maraslis, and T. Tryfonas, "Towards effective cybersecurity resource allocation: The Monte Carlo predictive modeling approach," *Int. J. Crit. Infrastruct.*, vol. 13, no. 2–3, pp. 152–167, 2017.
[33] J. Lewis and C. E. Turbyfill, "The how and why of cybersecurity policy: Create behavioral and technical rules to mitigate risk," *Cyber Secur. Peer-Rev. J.*, vol. 6, no. 2, pp. 132–140, 2022.
[34] A. Malin and G. Van Heule, "Continuous monitoring and cybersecurity for high-performance computing," in *Proc. 1st Workshop Changing Landscapes HPC Secur.*, 2013, pp. 9–14.
[35] K. Dempsey et al., *Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment*. NIST Spec. Publ. (SP) 800-137A (Withdrawn), Nat. Inst. Stand. Technol., 2020.

[36] W. He and Z. Zhang, "Enterprise cybersecurity training and awareness programs: Recommendations for success," *J. Organ. Comput. Electron. Commer.*, vol. 29, no. 4, pp. 249–257, 2019.
[37] I. Hamburg and K. R. Grosch, "Aligning a cybersecurity strategy with communication management in organisations," in *Digital Commun. Manage.*, IntechOpen, 2018, pp. 43–58.
[38] B. O. Omoyiola and J. Mckeeby, "Strategies for implementing cybersecurity policies in organisations (A case study of West African organisations)," *J. Cyber Secur. Res.*, vol. 8, no. 2, pp. 150–172, 2023.
[39] J. R. C. Nurse, "Cybersecurity risk communication: Understanding information trust and security usability," *IEEE Commun. Surv. Tutor.*, vol. 15, no. 4, pp. 1475–1490, 2013, doi: 10.1109/SURV.2013.013013.00142.
[40] I. Corradini, "Shaping cybersecurity awareness programs: Lessons from behavioral sciences," *Cyberpsychol. Behav. Soc. Netw.*, vol. 23, no. 5, pp. 333–341, 2020, doi: 10.1089/cyber.2019.0428.
[41] Nat. Inst. Stand. Technol., *Framework for Improving Critical Infrastructure Cybersecurity*, 2018.
[42] Eur. Union, *General Data Protection Regulation (EU GDPR)*, 2016.
[43] Afr. Union, *African Union Convention on Cybersecurity and Personal Data Protection*, 2014.
[44] Asia-Pac. Econ. Coop. (APEC), *APEC Framework for Securing the Digital Economy*, 2015.
[45] Int. Organ. Stand. (ISO), *ISO/IEC 27001:2022 Information Security Management Systems – Requirements*, 2022.