

A Cybersecurity Governance Framework for Strengthening Policy Compliance and Organizational Cybersecurity Management

Johnnecia Serwaa Agyemang
*College of Business and Management
Department of Cybersecurity Management
University of Illinois Springfield, Springfield, USA*

Bernice Buabeng
*College of Business and Information Systems
Department of Information Systems
Dakota State University*

Magdalene Kumi
Cybersecurity Analyst

Abstract

The growing reliance of organizations on digital technologies, cloud computing, information systems, and interconnected infrastructures has increased the need for effective cybersecurity governance and consistent adherence to organizational security policies. Despite the widespread adoption of cybersecurity policies and technical safeguards, organizations may continue to experience security weaknesses arising from inconsistent policy implementation, unclear accountability, inadequate security awareness, and insufficient compliance oversight. This study proposes a Cybersecurity Governance and Policy Compliance Framework that integrates organizational governance with the implementation, monitoring, and continuous improvement of cybersecurity policies. Using a qualitative conceptual research approach, the study synthesizes relevant academic literature, cybersecurity standards, and governance frameworks published between 2014 and 2026. The proposed framework comprises seven interrelated components: leadership and accountability, policy development, security awareness and training, policy implementation, compliance monitoring, corrective action, and continuous improvement. Its conceptual foundation draws on the NIST Cybersecurity Framework (CSF) 2.0, ISO/IEC 27001:2022, COBIT 2019, and contemporary research on information security policy compliance. In contrast to approaches that predominantly emphasize individual employee compliance behavior, this framework conceptualizes policy compliance as an organization-wide governance process involving leadership, clearly defined responsibilities, systematic oversight, and continuous evaluation. The proposed framework contributes to cybersecurity governance literature by providing an integrated structure for aligning governance responsibilities with policy implementation and compliance management. It also offers a practical foundation for organizations seeking to strengthen accountability, improve policy effectiveness, enhance compliance oversight, and support continuous improvement in cybersecurity management.

Keywords: *Cybersecurity Governance, Information Security Policy Compliance, Cybersecurity Management, Organizational Accountability, Security Awareness, Compliance Monitoring, Cybersecurity Policy, Information Security Management, Continuous Improvement*

Date of Submission: 02-10-2026

Date of Acceptance: 12-10-2026

I. INTRODUCTION

Cybersecurity has increasingly become an organizational management responsibility rather than a function limited to information technology departments. Organizations rely on digital systems to conduct business operations, store information, communicate with stakeholders, and provide services. Because of this, cybersecurity decisions must be integrated with organizational governance, risk management, policies, and accountability. The NIST Cybersecurity Framework (CSF) 2.0 emphasizes this broader perspective by introducing the Govern function and positioning cybersecurity risk as an organizational governance concern (Pascoe et al., 2024).

The establishment of cybersecurity policies is an important part of organizational security management. Policies define acceptable behavior, establish security responsibilities, and set requirements for employees to protect organizational information and technology resources. However, the existence of a policy does not guarantee compliance. Employees' compliance with information security policies can be influenced by factors such as socialization, social influence, employee capabilities, and competence (Ifinedo, 2014). Threat perceptions, self-efficacy, attitudes, and social norms are also relevant factors in employees' intention to comply with information security policies (Siponen et al., 2014).

Recent literature indicates that the policy compliance problem extends beyond individual employee behavior. A systematic literature review of information security policy compliance research identified a need for stronger approaches to evaluating compliance and incorporating organizational theories into compliance models (Alias, 2019). More recent research has continued to examine the combined influence of organizational and behavioral factors on security policy compliance (Amankwa et al., 2022). Information security policy compliance and violations are influenced by multiple factors, and the existing literature remains strongly focused on behavioral explanations (Balagopal & Mathew, 2024).

At the governance level, organizations have access to established frameworks that guide the management of cybersecurity and information technology. NIST CSF 2.0 provides cybersecurity outcomes that organizations can use to manage and reduce cybersecurity risk, while ISO/IEC 27001:2022 provides requirements for establishing, implementing, maintaining, and continually improving an information security management system. COBIT 2019 provides a broader governance and management framework for enterprise information and technology. These frameworks provide strong foundations, but organizations still need practical mechanisms for connecting governance responsibilities to policy implementation and employee compliance.

This study therefore proposes a Cybersecurity Governance and Policy Compliance Framework that connects organizational leadership and accountability with policy development, communication, implementation, monitoring, corrective action, and continuous improvement. The purpose is not to replace existing cybersecurity standards but to provide a conceptual governance structure that helps organizations translate cybersecurity policies into continuously managed organizational practices.

II. CONCEPTUAL RESEARCH APPROACH

This study adopts a qualitative conceptual research approach. Rather than collecting survey data or conducting statistical analysis, the study synthesizes findings from academic literature, cybersecurity standards, and established governance frameworks published from 2014 to 2026.

The literature was examined to identify recurring themes associated with cybersecurity governance and information security policy compliance, including leadership, accountability, policy development, employee awareness, organizational culture, monitoring, enforcement, and continuous improvement. Research on information security policy compliance was considered alongside established cybersecurity governance frameworks to identify areas where governance and compliance can be more directly connected.

The proposed framework draws particularly from NIST CSF 2.0, ISO/IEC 27001:2022, and COBIT 2019. NIST CSF 2.0 provides a flexible structure for managing cybersecurity risk across organizations and includes governance outcomes related to organizational context, strategy, roles, responsibilities, policies, and oversight (Pascoe et al., 2024). ISO/IEC 27001:2022 establishes requirements for an information security management system and emphasizes continual improvement. COBIT 2019 provides governance and management objectives and distinguishes governance activities from management activities.

The conceptual synthesis of these sources forms the basis for the framework proposed in this study.

III. LITERATURE REVIEW

3.1 Cybersecurity Governance in Organizations

Cybersecurity governance establishes the structures, responsibilities, policies, and oversight mechanisms through which organizations direct and manage cybersecurity activities. As organizations become increasingly dependent on digital technologies, cybersecurity can no longer be treated solely as a technical responsibility assigned to information technology departments. Cybersecurity incidents can affect organizational operations, financial performance, regulatory compliance, stakeholder confidence, and the protection of sensitive information. Consequently, cybersecurity governance requires participation from organizational leadership and integration with broader governance and enterprise risk management processes.

Effective cybersecurity governance begins with clearly defined leadership responsibilities and accountability. Senior leaders and governing bodies play an important role in establishing cybersecurity priorities, determining acceptable levels of risk, allocating appropriate resources, and ensuring that cybersecurity objectives support organizational goals. Management is responsible for translating these priorities into policies, procedures, controls, and operational practices. Clearly defined responsibilities are particularly important because cybersecurity activities frequently extend across multiple organizational functions, including information

technology, human resources, legal and compliance departments, risk management, operations, and senior leadership. Without clearly established responsibilities, organizations may experience gaps in accountability, inconsistent policy implementation, and inadequate responses to identified security risks.

The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) 2.0 reinforces the importance of cybersecurity governance by introducing Govern as a distinct function alongside Identify, Protect, Detect, Respond, and Recover. The Govern function focuses on establishing and monitoring an organization's cybersecurity risk management strategy, expectations, and policy (Pascoe et al., 2024). Its inclusion reflects the recognition that governance activities influence how organizations implement the other cybersecurity functions. Governance therefore provides the organizational foundation for determining cybersecurity priorities, assigning responsibilities, establishing policies, overseeing risk management activities, and evaluating cybersecurity performance.

An important contribution of NIST CSF 2.0 is its emphasis on connecting cybersecurity risk management with enterprise risk management. Cybersecurity risks do not exist independently of other organizational risks. A cyber incident may interrupt operations, compromise confidential information, create financial losses, affect regulatory compliance, and damage organizational reputation. For this reason, cybersecurity risk should be considered within broader organizational decision-making processes. Integrating cybersecurity with enterprise risk management enables leadership to evaluate cybersecurity priorities in relation to organizational objectives, available resources, regulatory obligations, and stakeholder expectations. This integration can also improve communication between technical security personnel and organizational decision-makers by establishing a common governance structure for understanding and managing cybersecurity risk.

COBIT 2019 provides an additional governance perspective by distinguishing governance responsibilities from management responsibilities. Within COBIT, governance involves evaluating stakeholder needs and organizational conditions, establishing direction through prioritization and decision-making, and monitoring organizational performance and compliance. Management, in contrast, plans, builds, operates, and monitors activities in accordance with the direction established by the governing body (ISACA, 2019). This distinction is important for cybersecurity because effective security management requires both strategic direction and operational execution. Leadership may establish cybersecurity objectives and expectations, while management and operational personnel implement the processes and controls required to achieve those objectives.

COBIT 2019 also demonstrates that effective governance depends on more than formal organizational structures. Its governance system incorporates interconnected components that include processes, organizational structures, policies and procedures, information flows, culture and behaviors, people and skills, and technological infrastructure (ISACA, 2019). These components are particularly relevant to cybersecurity policy compliance. A cybersecurity policy may establish appropriate requirements, but implementation can remain ineffective if employees are not adequately trained, responsibilities are unclear, organizational culture does not support security practices, or compliance is not monitored. Cybersecurity governance must therefore address both formal policy requirements and the organizational conditions necessary to support their implementation.

ISO/IEC 27001:2022 provides another important foundation for organizational cybersecurity governance through its requirements for an information security management system (ISMS). The standard supports a systematic approach to establishing, implementing, maintaining, and continually improving information security management (International Organization for Standardization, 2022). Through an ISMS, organizations can establish information security objectives, assess risks, implement appropriate controls, evaluate performance, and address areas requiring improvement. The emphasis on continual improvement is particularly relevant because cybersecurity risks, technologies, regulatory requirements, and organizational environments continually evolve. Cybersecurity governance therefore requires mechanisms that enable organizations to evaluate existing practices and adapt their policies and controls when circumstances change.

Although NIST CSF 2.0, COBIT 2019, and ISO/IEC 27001:2022 differ in their structures and purposes, they share several important governance principles. Each recognizes the importance of organizational leadership, clearly established responsibilities, risk-based decision-making, policies, monitoring, and continuous evaluation. NIST CSF 2.0 provides a flexible cybersecurity risk management structure, COBIT 2019 provides a broader governance and management framework for enterprise information and technology, and ISO/IEC 27001:2022 establishes requirements for a systematic information security management system. Rather than functioning as competing approaches, these frameworks can provide complementary perspectives for understanding organizational cybersecurity governance.

The relationship between governance and cybersecurity policy compliance is particularly important. Governance establishes organizational expectations and assigns responsibility, while cybersecurity policies translate these expectations into requirements that guide employee and organizational behavior. However, policy effectiveness depends on more than the existence of formally documented requirements. Organizations must communicate policies, provide appropriate awareness and training, establish mechanisms for implementation, monitor compliance, respond to noncompliance, and periodically review whether policies remain appropriate for

emerging risks and organizational needs. These activities demonstrate that policy compliance can be understood as part of a broader governance process rather than solely as an issue of individual employee behavior.

Effective cybersecurity governance requires a continuous relationship among leadership, policy development, implementation, oversight, and improvement. Organizational leaders establish direction and accountability; policies translate that direction into security expectations; employees and managers implement those expectations; monitoring processes evaluate compliance and effectiveness; and corrective actions address identified weaknesses. Lessons from monitoring and corrective actions can subsequently inform revisions to policies and governance priorities. This continuous process provides the conceptual foundation for connecting cybersecurity governance with policy compliance and supports the development of the Cybersecurity Governance and Policy Compliance Framework proposed in this study.

3.2 Cybersecurity Policy Compliance

Cybersecurity policies are an important component of organizational cybersecurity management because they establish expectations regarding the protection, access, and appropriate use of information systems and resources. These policies provide employees with guidance on acceptable security practices and define responsibilities for protecting organizational information. They may address areas such as access control, password management, data protection, acceptable use of organizational systems, incident reporting, remote access, and the handling of sensitive information. However, the existence of formally documented cybersecurity policies does not necessarily ensure that employees understand or consistently follow established requirements. The effectiveness of a cybersecurity policy ultimately depends on how successfully its requirements are communicated, implemented, supported, and monitored throughout the organization.

Research on information security policy compliance has traditionally placed considerable emphasis on understanding the factors that influence employees' security behavior. Employees may differ in their knowledge of cybersecurity requirements, perceptions of security threats, confidence in performing required security practices, and willingness to follow organizational policies. Ifinedo (2014) demonstrated that factors such as socialization, social influence, and employees' capabilities can contribute to information security policy compliance. These findings indicate that compliance is influenced not only by the existence of formal rules but also by the social and organizational environment in which employees perform their responsibilities.

Similarly, Siponen et al. (2014) identified several factors associated with employees' intentions to comply with information security policies, including threat perceptions, self-efficacy, attitudes, and social norms. Employees who recognize the potential consequences of cybersecurity threats and believe that they are capable of performing appropriate security practices may be more willing to comply with organizational requirements. Social expectations within the workplace can also influence security behavior because employees frequently observe how supervisors and colleagues respond to organizational policies. Consequently, cybersecurity policy compliance is partly shaped by the interaction between individual perceptions and the organizational environment.

These findings demonstrate that policy compliance cannot be achieved simply by developing and distributing cybersecurity policies. Employees must understand what is expected of them, recognize the relevance of cybersecurity requirements to their responsibilities, and possess the knowledge and skills necessary to perform required security practices. Policies that are overly complex, poorly communicated, or disconnected from employees' daily responsibilities may be difficult to implement consistently. Organizations therefore need mechanisms for communicating policy requirements in understandable terms and ensuring that employees receive appropriate cybersecurity awareness and training.

Security awareness and training are particularly important because cybersecurity policies frequently require employees to make security-related decisions during routine organizational activities. Employees may be expected to identify suspicious communications, protect authentication credentials, appropriately handle sensitive information, report security incidents, or follow established procedures when accessing organizational systems. Awareness initiatives can help employees understand why these requirements exist, while training can provide the practical knowledge necessary to apply them. However, awareness and training should not be viewed as isolated activities. They should form part of a broader organizational process in which cybersecurity expectations are reinforced through leadership, communication, supervision, and ongoing evaluation.

The organizational environment can further influence whether cybersecurity requirements are consistently followed. Employees operate within organizational structures that establish priorities, allocate resources, define responsibilities, and determine how policies are enforced. When cybersecurity expectations are supported by management and integrated into routine organizational processes, employees may have clearer guidance regarding their responsibilities. In contrast, unclear accountability, inconsistent communication, inadequate resources, or conflicting organizational priorities may create conditions in which security policies are difficult to implement. Policy compliance should therefore be considered in relation to both employee behavior and the organizational mechanisms that shape that behavior.

Research on information security policy compliance has highlighted the need for stronger approaches to evaluating compliance and for greater consideration of organizational factors. Alias (2019) identified

opportunities for compliance research to incorporate broader organizational perspectives and improve approaches to evaluating information security policy compliance. This suggests that understanding why individual employees comply or fail to comply with policies represents only one dimension of the compliance problem. Organizations must also consider whether appropriate governance structures, communication processes, monitoring mechanisms, and accountability arrangements exist to support compliance.

More recent research has reinforced the importance of considering multiple influences on information security policy compliance. Amankwa et al. (2022) examined factors affecting employees' compliance with information security policies and demonstrated that compliance is influenced by organizational as well as individual considerations. Similarly, Balagopal and Mathew (2024) indicate that information security policy compliance and violations involve multiple interacting factors rather than a single behavioral explanation. Collectively, these findings demonstrate the complexity of cybersecurity policy compliance and support the need for approaches that consider the relationship between individual behavior and the broader organizational environment.

Another important aspect of policy compliance is monitoring. Organizations need mechanisms for determining whether established cybersecurity requirements are being followed and whether existing policies remain effective. Monitoring may include compliance reviews, security assessments, internal audits, incident analysis, access reviews, and other forms of organizational oversight. The purpose of such activities should extend beyond identifying violations. Monitoring can also reveal unclear policy requirements, inadequate training, implementation difficulties, emerging risks, or weaknesses in organizational processes. These findings can provide valuable information for improving both cybersecurity policies and the governance mechanisms that support them.

Corrective action is therefore an important component of effective policy compliance management. When noncompliance or policy weaknesses are identified, organizations should determine the underlying causes and implement appropriate responses. Depending on the circumstances, corrective measures may include additional training, clarification of policy requirements, modification of procedures, adjustment of technical controls, reassignment of responsibilities, or other appropriate organizational actions. This approach recognizes that noncompliance may result from different causes and that effective responses should address the specific factors contributing to the problem.

Cybersecurity policy compliance should consequently be viewed as a continuous organizational process rather than a one-time employee obligation. Policies must be developed and communicated, employees must receive appropriate awareness and training, implementation must be supported, compliance must be monitored, identified weaknesses must be addressed, and policies must be periodically reviewed as organizational conditions and cybersecurity risks evolve. This continuous process connects employee compliance with broader cybersecurity governance responsibilities.

Accordingly, an effective approach to cybersecurity policy compliance requires the integration of behavioral and organizational perspectives. Employee knowledge, attitudes, capabilities, and perceptions remain important, but these factors operate within governance structures established by organizational leadership. Leadership commitment, clearly defined responsibilities, effective communication, appropriate training, systematic monitoring, corrective action, and continuous improvement can collectively create an environment that supports consistent policy implementation. Viewing policy compliance from this broader perspective provides an important foundation for connecting cybersecurity governance with policy compliance and supports the development of the Cybersecurity Governance and Policy Compliance Framework proposed in this study.

3.3 Security Awareness, Communication, and Accountability

Security awareness, effective communication, and clearly defined accountability are essential components of cybersecurity policy implementation. While cybersecurity policies establish organizational expectations and requirements, their effectiveness depends substantially on whether employees understand those requirements and recognize their individual responsibilities. Employees cannot be expected to consistently comply with security requirements that are unclear, poorly communicated, or disconnected from their daily responsibilities. Consequently, organizations must establish mechanisms that translate formal cybersecurity policies into understandable and actionable security practices.

Security awareness provides an important connection between organizational cybersecurity policies and employee behavior. Awareness initiatives help employees understand the cybersecurity risks associated with organizational activities and the potential consequences of inappropriate security practices. Employees routinely interact with information systems, organizational data, email platforms, cloud applications, authentication systems, and other digital resources. These interactions can expose organizations to cybersecurity risks when employees are unaware of established requirements or do not understand how those requirements should be applied. Security awareness therefore contributes to policy compliance by increasing employees' understanding of both cybersecurity risks and their responsibilities for reducing those risks.

However, cybersecurity awareness should extend beyond the general distribution of security information. Effective awareness programs should communicate why cybersecurity requirements are important, how employees' actions can affect organizational security, and what specific behaviors are expected in different situations. For example, employees may need to understand how to identify suspicious communications, protect authentication credentials, appropriately handle sensitive information, report potential security incidents, and use organizational systems in accordance with established policies. Providing this information in practical and understandable terms can help employees connect formal policy requirements with their routine work activities.

Communication is therefore a critical element of cybersecurity policy implementation. Policies that are technically comprehensive may still be ineffective when their requirements are not clearly communicated to the individuals responsible for implementing them. Organizations should communicate cybersecurity expectations through appropriate channels and ensure that employees understand how policies apply to their specific roles. Communication may occur through formal policy documents, employee orientation, security awareness programs, training sessions, internal communications, managerial guidance, and periodic security reminders. Using multiple communication mechanisms can reinforce organizational expectations and provide employees with continuing opportunities to understand cybersecurity responsibilities.

The relevance of cybersecurity communication is also important. Employees perform different functions and may face different security risks depending on their organizational roles. Consequently, security awareness and training should not rely exclusively on standardized information provided uniformly to all employees. General cybersecurity awareness can establish a common foundation, but role-specific training can help employees understand the security requirements most relevant to their responsibilities. Employees responsible for financial transactions, human resources, information technology, customer information, or administrative functions, for example, may require different forms of security guidance. Aligning training with employees' actual activities can make cybersecurity requirements more meaningful and applicable to everyday work.

Security awareness should also be viewed as a continuous process rather than a one-time activity. Cybersecurity threats, organizational technologies, policies, and work practices change over time. Employees who receive security training only when they join an organization may not remain adequately informed about emerging risks or revised policy requirements. Periodic awareness activities and updated training can reinforce established expectations while introducing employees to changes in organizational security practices. Continuous communication can also help maintain cybersecurity as an ongoing organizational priority rather than an issue addressed only after a security incident occurs.

Although awareness and communication are necessary, they are unlikely to produce consistent policy compliance without clearly defined accountability. Accountability establishes responsibility for cybersecurity activities and helps ensure that individuals understand the security obligations associated with their roles. At the employee level, individuals should understand the policies and procedures they are expected to follow, the security practices associated with their responsibilities, and the appropriate mechanisms for reporting security concerns or incidents. Clear expectations reduce ambiguity and provide a foundation for evaluating compliance.

Accountability, however, should not be limited to employees. Managers and organizational leaders also have important cybersecurity responsibilities. Leadership is responsible for establishing appropriate governance structures, approving and supporting cybersecurity policies, allocating resources, and demonstrating organizational commitment to cybersecurity. Managers contribute by communicating expectations, supporting employee training, supervising policy implementation, and addressing identified compliance problems. Cybersecurity and information technology personnel may be responsible for implementing technical safeguards and providing specialized guidance, while risk, compliance, human resources, and other organizational functions may contribute to policy development, monitoring, and enforcement. Clearly defining these responsibilities can reduce gaps in policy implementation and strengthen coordination across organizational functions.

Leadership behavior can also influence how employees perceive cybersecurity requirements. When organizational leaders consistently communicate the importance of cybersecurity and demonstrate support for established policies, employees may be more likely to view cybersecurity as an organizational priority. Conversely, when formal security requirements conflict with managerial practices or operational expectations, employees may receive inconsistent messages about the importance of compliance. Leadership commitment should therefore be demonstrated not only through formal policy approval but also through resource allocation, communication, oversight, and consistent support for cybersecurity practices.

Recent research further suggests that information security policy compliance is influenced by organizational and social factors in addition to individual knowledge. Factors such as trust in management, psychological ownership, social influence, security awareness, and self-efficacy may contribute to employees' willingness to comply with information security requirements (Alshammari & Al-Mamary, 2026). These factors illustrate that employee security behavior develops within a broader organizational environment. Employees' perceptions of leadership, workplace expectations, organizational relationships, and their own ability to perform required security practices can interact with formal cybersecurity policies and influence compliance behavior.

Trust in management is particularly relevant to cybersecurity communication and accountability. Employees may be more receptive to security requirements when they perceive that organizational leaders communicate expectations consistently and implement policies in a credible manner. Similarly, social influence can shape employees' perceptions of acceptable security behavior because individuals may observe and respond to the practices of supervisors and colleagues. When secure behavior is reinforced throughout the organization, compliance can become part of established workplace expectations rather than simply an individual obligation.

Self-efficacy also has practical implications for cybersecurity awareness and training. Employees may understand that a particular security behavior is important but still lack confidence in their ability to perform it correctly. Effective training should therefore provide employees with practical knowledge and opportunities to understand how security requirements apply in realistic situations. Strengthening employees' ability to perform expected security practices can complement policy communication and reduce the gap between awareness and implementation.

These considerations demonstrate that security awareness, communication, and accountability are closely interconnected. Awareness helps employees recognize cybersecurity risks and understand expected behaviors; communication translates organizational policies into accessible and role-relevant guidance; and accountability clarifies responsibility for implementing and overseeing cybersecurity requirements. Weakness in any one of these areas can undermine policy implementation. For example, clearly defined responsibilities may have limited value when employees do not understand the relevant policy, while comprehensive awareness training may have limited impact when managers do not reinforce organizational expectations or monitor compliance.

From a governance perspective, organizations should therefore integrate awareness, communication, and accountability into a continuous cybersecurity management process. Leadership should establish cybersecurity expectations and assign responsibilities; policies should communicate those expectations; awareness and training should provide employees with the knowledge and skills required for implementation; and managers should reinforce and monitor compliance. Information obtained through monitoring, employee feedback, security incidents, and compliance reviews can subsequently identify areas where additional communication, training, or clarification of responsibilities is necessary.

Integrating these elements supports the broader view that cybersecurity policy compliance is an organizational governance responsibility rather than solely an individual employee obligation. Employees remain responsible for following established requirements, but organizational leaders and managers are responsible for creating conditions that enable and reinforce appropriate security behavior. Security awareness, effective communication, and clearly defined accountability therefore provide an essential link between governance expectations and practical policy implementation. These relationships form an important component of the Cybersecurity Governance and Policy Compliance Framework proposed in this study.

3.4 Compliance Monitoring and Continuous Improvement

Cybersecurity policy compliance requires continuous monitoring because organizational systems, technologies, workforce practices, regulatory requirements, and cyber threats change over time. A cybersecurity policy that was appropriate when initially developed may become less effective as new technologies are introduced, organizational responsibilities change, or new security risks emerge. Organizations should therefore periodically evaluate both employee compliance with established requirements and the continued effectiveness of the policies themselves. Monitoring provides the information necessary to identify weaknesses, evaluate implementation, and determine whether existing cybersecurity practices remain aligned with organizational objectives and risk conditions.

Compliance monitoring can involve multiple organizational activities, including internal audits, security assessments, access reviews, incident analysis, policy reviews, risk assessments, technical monitoring, and evaluation of employee security practices. These activities can provide evidence regarding whether cybersecurity requirements are being implemented consistently and whether existing controls are achieving their intended objectives. Monitoring can also identify differences between formally established policies and actual organizational practices. Such differences are important because a policy may appear comprehensive when documented but remain ineffective if its requirements are difficult to implement or are not consistently followed.

NIST CSF 2.0 supports this continuous approach by providing cybersecurity outcomes that organizations can use to understand and assess their cybersecurity risk management activities. Organizations can use CSF Profiles to describe current and target cybersecurity postures, helping them identify gaps between existing practices and desired outcomes. The NIST CSF 2.0 Tiers also characterize the rigor of an organization's cybersecurity risk governance and management practices and can provide context for understanding how cybersecurity risk is managed across an organization (Quinn et al., 2024). These mechanisms support ongoing evaluation by enabling organizations to examine their existing cybersecurity practices and identify opportunities for improvement.

ISO/IEC 27001:2022 similarly emphasizes continual improvement as an important element of an information security management system. Under this approach, information obtained from monitoring, measurement, audits, management reviews, risk assessments, and security incidents can contribute to improvements in information security management. Continual improvement recognizes that cybersecurity management is not a static activity. Instead, organizations must periodically evaluate their security practices and make adjustments in response to changing risks, technologies, business processes, regulatory requirements, and lessons learned from previous security events.

Compliance monitoring should therefore function as more than a mechanism for identifying employee violations. It should serve as a feedback process through which organizations evaluate both individual compliance and the effectiveness of the organizational conditions supporting policy implementation. When noncompliance is identified, organizations should examine why the violation occurred rather than assuming that it resulted solely from an employee's unwillingness to follow established requirements. Potential causes may include insufficient security awareness, unclear or overly complex policy requirements, inadequate training, limited resources, conflicting work demands, technical limitations, or insufficient management support.

Identifying the underlying cause of noncompliance is important because different causes require different corrective responses. For example, noncompliance resulting from limited employee understanding may require additional training or clearer communication. If employees understand a policy but lack the technological resources necessary to comply, the organization may need to modify systems or provide additional resources. Similarly, repeated noncompliance across multiple departments may indicate weaknesses in policy design, management oversight, or organizational processes rather than isolated employee behavior. A systematic approach to corrective action allows organizations to address these underlying conditions and reduce the likelihood that similar problems will recur.

Corrective action should consequently be connected to organizational learning and policy improvement. Findings from audits, incidents, employee feedback, risk assessments, and compliance monitoring can be used to determine whether existing policies require clarification, modification, or replacement. Organizations may also identify the need for revised training programs, additional technical controls, clearer assignment of responsibilities, or stronger management oversight. In this way, monitoring produces information that can be incorporated into future governance and policy decisions.

Continuous improvement completes this feedback process by returning lessons from monitoring and corrective action to the governance level. Organizational leaders can use this information to reassess cybersecurity priorities, allocate resources, revise policies, strengthen accountability, and establish new security objectives when necessary. Updated policies can then be communicated and implemented, followed by further monitoring and evaluation. This creates a continuous cycle in which cybersecurity governance and policy compliance evolve in response to organizational experience and changing risk conditions.

Accordingly, compliance monitoring and continuous improvement provide an essential connection between policy implementation and cybersecurity governance. Monitoring identifies whether established requirements are being followed and whether existing practices remain effective; corrective action addresses identified weaknesses; and continuous improvement ensures that lessons learned contribute to future cybersecurity decisions. Incorporating this feedback process into cybersecurity governance supports a more adaptive approach to policy compliance and represents a central component of the Cybersecurity Governance and Policy Compliance Framework proposed in this study.

IV. RESEARCH GAP

The existing literature provides substantial insight into information security and cybersecurity policy compliance. A significant portion of this research has focused on understanding the factors that influence employees' decisions to comply with or violate organizational security policies. Behavioral and social perspectives, including Protection Motivation Theory, the Theory of Planned Behavior, deterrence perspectives, and social influence approaches, have contributed to explaining how individual attitudes, threat perceptions, self-efficacy, social expectations, and related behavioral factors may influence policy compliance (Ifinedo, 2014; Siponen et al., 2014). These studies have provided an important foundation for understanding the human dimension of organizational cybersecurity.

Despite these contributions, an emphasis on individual compliance behavior does not fully explain how organizations establish and maintain effective cybersecurity policy compliance. Employees operate within organizational environments shaped by leadership priorities, management practices, organizational culture, resource availability, communication processes, technological capabilities, and accountability structures. Research has demonstrated that organizational and behavioral factors can jointly influence the development of an information security policy compliance culture (Amankwa et al., 2022). Consequently, policy compliance should be considered not only in terms of employees' willingness or intention to follow security requirements but also in relation to the organizational mechanisms that support and reinforce those requirements.

Research examining organizational influences on information security policy compliance has begun to address this broader perspective. Factors such as management support, security awareness, organizational culture, social influence, employee capabilities, and accountability have increasingly been considered alongside individual behavioral factors (Amankwa et al., 2022). Nevertheless, a systematic review of information security policy compliance research identified limitations in approaches for evaluating compliance and emphasized the need to strengthen compliance models through greater incorporation of organizational theories (Angraini et al., 2019). These findings create an opportunity to conceptualize policy compliance more broadly by examining how governance structures and organizational processes collectively support policy development, implementation, monitoring, and improvement.

At the same time, established cybersecurity and information technology governance frameworks provide extensive guidance for managing cybersecurity risk. NIST CSF 2.0 emphasizes cybersecurity governance through the Govern function and provides outcomes related to organizational context, risk management strategy, roles, responsibilities, authorities, policies, oversight, and cybersecurity supply chain risk management (National Institute of Standards and Technology [NIST], 2024). ISO/IEC 27001:2022 provides requirements for establishing, implementing, maintaining, and continually improving an information security management system (International Organization for Standardization [ISO], 2022). COBIT 2019 provides a broader framework for the governance and management of enterprise information and technology and distinguishes governance responsibilities from management activities (ISACA, 2019). Collectively, these frameworks establish important foundations for cybersecurity governance, risk management, accountability, and organizational oversight.

However, these established frameworks serve broader purposes than explaining the organizational process through which cybersecurity policy compliance is achieved and sustained. NIST CSF 2.0 provides cybersecurity outcomes that organizations can use to understand and manage cybersecurity risk rather than functioning specifically as a behavioral model of employee policy compliance (NIST, 2024). ISO/IEC 27001:2022 establishes requirements for an information security management system and continual improvement rather than providing a behavioral explanation of employee compliance (ISO, 2022). Similarly, COBIT 2019 provides comprehensive governance and management objectives for enterprise information and technology rather than focusing specifically on the behavioral determinants of cybersecurity policy compliance (ISACA, 2019).

This distinction reveals an important conceptual opportunity between two established areas of knowledge. On one side, information security policy compliance research provides detailed explanations of behavioral, cognitive, and social factors influencing employees' security practices (Ifinedo, 2014; Siponen et al., 2014). On the other side, cybersecurity and information security governance frameworks provide organizational structures and processes for directing, managing, and overseeing cybersecurity and information security risks (ISACA, 2019; ISO, 2022; NIST, 2024). Greater conceptual integration between these perspectives could help explain how governance responsibilities systematically support policy compliance from policy development through implementation, monitoring, corrective action, and continuous improvement.

A further opportunity concerns the treatment of policy compliance as a continuous organizational process. Measuring employees' intentions to comply and examining the factors associated with those intentions provide valuable information about security behavior (Ifinedo, 2014; Siponen et al., 2014). However, organizations must also determine how policies are developed, communicated, implemented, evaluated, and revised over time. The systematic review by Angraini et al. (2019) identified a need for stronger approaches to evaluating information security policy compliance, while organizational compliance research demonstrates the importance of considering organizational and behavioral factors together (Amankwa et al., 2022). These findings support a broader approach in which compliance is incorporated into an ongoing organizational governance process.

The literature reviewed in this study therefore suggests the need for a more integrated conceptual approach connecting organizational governance mechanisms with the practical cybersecurity policy-compliance lifecycle. Such an approach should recognize that responsibility for compliance extends across multiple organizational levels. Leadership establishes strategic direction and accountability; managers translate governance expectations into operational practices; cybersecurity and information technology personnel support implementation and monitoring; and employees apply security requirements during routine organizational activities. Compliance outcomes can consequently be understood as resulting from interactions among individual behavior, organizational conditions, and governance mechanisms rather than employee behavior alone (Amankwa et al., 2022; Angraini et al., 2019).

Another important opportunity involves connecting compliance monitoring with organizational learning and continuous improvement. NIST CSF 2.0 supports the assessment of cybersecurity outcomes and the identification of opportunities for improving cybersecurity risk management practices (NIST, 2024). CSF Organizational Profiles can be used to describe current and target cybersecurity postures, while CSF Tiers characterize the rigor of cybersecurity risk governance and management practices and can support the evaluation of improvement over time (Pascoe et al., 2024; Quinn et al., 2024). ISO/IEC 27001:2022 similarly incorporates continual improvement into information security management (ISO, 2022). These principles provide a foundation

for treating compliance monitoring as a feedback mechanism through which organizations can identify weaknesses and strengthen future policies and security practices.

Accordingly, this study addresses the identified conceptual gap by proposing a Cybersecurity Governance and Policy Compliance Framework that integrates seven interconnected components: leadership and accountability, policy development, security awareness and communication, policy implementation, compliance monitoring, corrective action, and continuous improvement. These components are derived from the synthesis of information security policy compliance research and established cybersecurity governance and information security management principles (Amankwa et al., 2022; Angraini et al., 2019; ISACA, 2019; ISO, 2022; NIST, 2024).

The proposed framework does not seek to replace NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019, or existing behavioral models of information security policy compliance. Instead, it provides a conceptual bridge between these perspectives. Behavioral research remains important for understanding employee security decisions (Ifinedo, 2014; Siponen et al., 2014), while established standards and frameworks provide guidance for cybersecurity governance, information security management, and organizational oversight (ISACA, 2019; ISO, 2022; NIST, 2024). The proposed framework builds on these contributions by illustrating how governance responsibilities can relate to the organizational processes required to establish, communicate, implement, monitor, and continuously improve cybersecurity policy compliance.

Through this integration, the study conceptualizes cybersecurity policy compliance not solely as an individual behavioral outcome but as an organization-wide governance outcome. This perspective distributes responsibility for effective compliance across leadership, management, cybersecurity functions, and employees and emphasizes the continuous interaction among governance, policy implementation, monitoring, corrective action, and organizational learning. Addressing this conceptual gap provides the foundation for the Cybersecurity Governance and Policy Compliance Framework presented in the following section.

V. PROPOSED CYBERSECURITY GOVERNANCE AND POLICY COMPLIANCE FRAMEWORK

The proposed Cybersecurity Governance and Policy Compliance Framework conceptualizes cybersecurity policy compliance as a continuous organizational governance process rather than as a one-time policy, training activity, or individual employee responsibility. The framework integrates principles derived from cybersecurity governance and information security management frameworks with findings from information security policy compliance research. It consists of seven interconnected components: (1) leadership and accountability, (2) policy development and alignment, (3) communication and security awareness, (4) policy implementation, (5) compliance monitoring and assessment, (6) corrective action and enforcement, and (7) continuous improvement. Together, these components establish a continuous cycle through which organizations can develop, implement, evaluate, and improve cybersecurity policies.

The first component, leadership and accountability, establishes the governance foundation for the framework. Organizational leaders are responsible for establishing cybersecurity expectations, defining responsibilities and authorities, allocating appropriate resources, and ensuring that cybersecurity priorities are aligned with organizational objectives. This emphasis is consistent with NIST CSF 2.0, which places governance at the center of cybersecurity risk management through its Govern function and addresses organizational context, risk management strategy, roles, responsibilities, policies, and oversight (National Institute of Standards and Technology [NIST], 2024). COBIT 2019 similarly emphasizes governance responsibilities involving the evaluation of stakeholder needs, establishment of organizational direction, and monitoring of organizational performance (ISACA, 2019). Within the proposed framework, leadership commitment provides the organizational authority and resources necessary to support all subsequent stages of policy compliance.

The second component is policy development and alignment. Cybersecurity policies should reflect the organization's objectives, cybersecurity risks, regulatory and legal obligations, technological environment, and operational requirements. Policies should also clearly define expected security practices and establish responsibilities for implementation and compliance. Alignment is important because cybersecurity policies that are disconnected from organizational operations may be difficult to implement consistently. NIST CSF 2.0 recognizes policy as an important governance outcome, while ISO/IEC 27001:2022 emphasizes the establishment and maintenance of information security policies within an information security management system (International Organization for Standardization [ISO], 2022; NIST, 2024). The proposed framework therefore positions policy development as a governance activity that translates organizational cybersecurity objectives into defined requirements.

The third component, communication and security awareness, connects formal cybersecurity policies with employee understanding and behavior. Developing a policy does not ensure that employees understand its requirements or recognize how those requirements apply to their responsibilities. Research has demonstrated that information security policy compliance can be influenced by factors such as social influence, employee

capabilities, threat perceptions, self-efficacy, attitudes, and social norms (Ifinedo, 2014; Siponen et al., 2014). Organizations should therefore communicate cybersecurity requirements clearly and provide awareness and training activities that are appropriate to employees' roles. General cybersecurity awareness can establish common expectations, while role-specific training can help employees understand how security requirements apply to their routine activities.

The fourth component is policy implementation. At this stage, formally established cybersecurity requirements are incorporated into organizational processes, technological systems, and employee activities. Effective implementation may require a combination of administrative, technical, and organizational controls. Examples include access management procedures, authentication requirements, data-handling processes, incident-reporting mechanisms, employee responsibilities, and supervisory practices. Implementation should also consider whether employees possess the resources, knowledge, authority, and technological capabilities necessary to comply with established requirements. This is important because noncompliance may result not only from individual choices but also from organizational conditions that make compliance difficult. Research examining information security policy compliance supports consideration of both behavioral and organizational factors when evaluating security practices (Amankwa et al., 2022; Angraini et al., 2019).

The fifth component, compliance monitoring and assessment, determines whether cybersecurity policies are being implemented as intended and whether established requirements remain effective. Monitoring may include internal audits, security assessments, access reviews, incident analysis, risk assessments, policy reviews, and evaluation of employee security practices. The purpose of monitoring is not limited to identifying violations. It also provides organizations with information about weaknesses in policy design, communication, implementation, training, resources, and organizational oversight. NIST CSF 2.0 supports the assessment of cybersecurity outcomes through mechanisms such as Organizational Profiles and CSF Tiers, which can assist organizations in evaluating cybersecurity risk management practices and identifying opportunities for improvement (NIST, 2024; Quinn et al., 2024).

The sixth component is corrective action and enforcement. When compliance monitoring identifies deficiencies, organizations should determine the underlying causes before selecting an appropriate response. Noncompliance may result from insufficient employee awareness, unclear policy requirements, inadequate training, technological limitations, insufficient resources, conflicting operational priorities, or deliberate violations. Corrective actions should therefore correspond to the nature and cause of the identified problem. Appropriate responses may include additional training, clarification or revision of policy requirements, changes to organizational processes, implementation or modification of technical controls, increased management intervention, or disciplinary measures where appropriate. This approach enables organizations to address underlying weaknesses rather than focusing exclusively on the immediate instance of noncompliance.

The seventh component, continuous improvement, completes the governance cycle. Cybersecurity policies and compliance mechanisms should evolve as organizational risks, technologies, legal requirements, regulatory expectations, and threat environments change. ISO/IEC 27001:2022 emphasizes continual improvement as a fundamental element of information security management (ISO, 2022). Within the proposed framework, information obtained from compliance monitoring, audits, cybersecurity incidents, risk assessments, employee feedback, and corrective actions is returned to organizational leadership and policy decision-making processes. These findings can inform revisions to policies, training programs, technical controls, resource allocation, accountability structures, and governance priorities.

An important characteristic of the proposed framework is the feedback relationship among its components. Although the framework can be represented as a sequence, its operation is not strictly linear. Findings from compliance monitoring may reveal weaknesses in employee awareness, policy design, implementation, or leadership oversight. Corrective action may therefore require returning to an earlier component of the framework. Similarly, changes in organizational objectives, regulations, technologies, or cybersecurity risks may require leadership to reassess priorities and initiate revisions to existing policies. Continuous improvement consequently feeds information back into leadership, accountability, and policy development, allowing the governance cycle to begin again under updated organizational conditions.

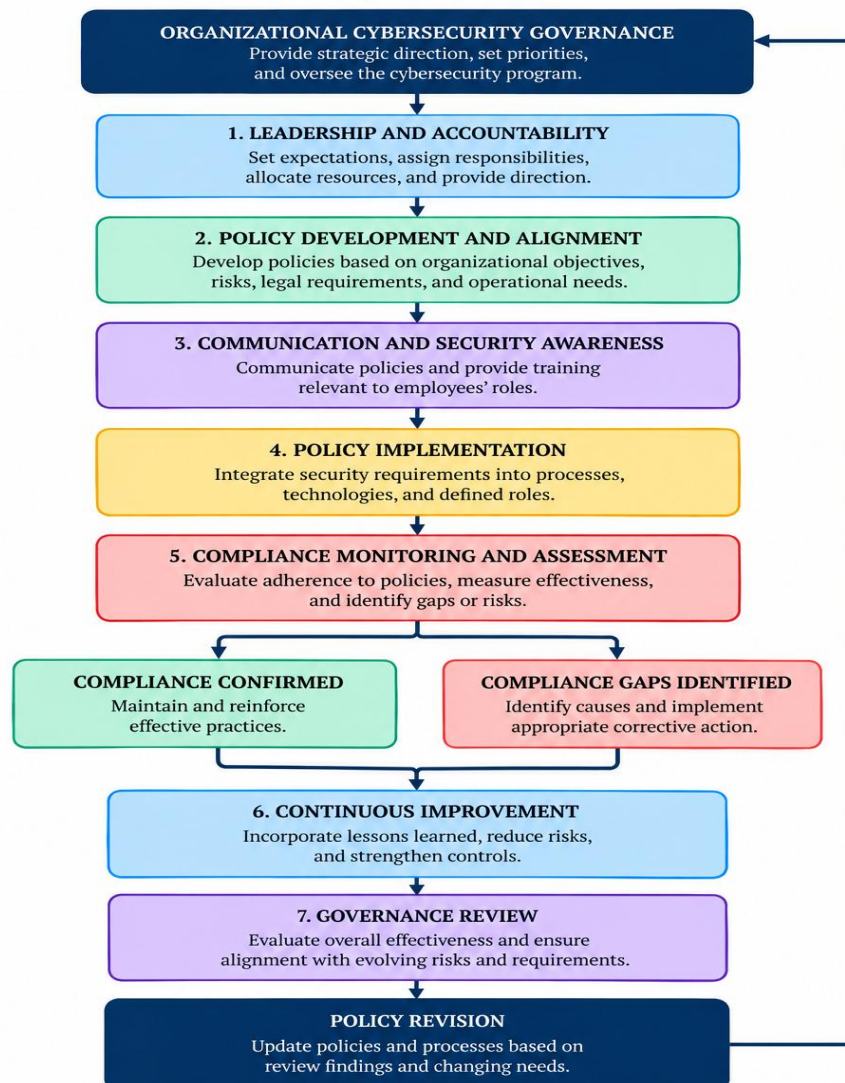
The framework also distributes responsibility for cybersecurity policy compliance across different organizational levels. Leadership establishes strategic direction and accountability; managers support implementation and oversight; cybersecurity and information technology personnel provide technical and operational support; and employees apply cybersecurity requirements during their daily activities. This distribution of responsibility reflects the broader view that cybersecurity policy compliance is influenced by interactions among individual behavior, organizational conditions, and governance mechanisms (Amankwa et al., 2022; Angraini et al., 2019).

The primary contribution of the proposed framework is therefore the integration of governance responsibilities with the cybersecurity policy-compliance lifecycle. Existing behavioral research provides valuable explanations of factors influencing employees' compliance decisions (Ifinedo, 2014; Siponen et al., 2014), while established frameworks provide guidance for cybersecurity governance and information security

management (ISACA, 2019; ISO, 2022; NIST, 2024). The proposed framework connects these perspectives by positioning policy compliance within a continuous organizational process involving leadership, policy development, awareness, implementation, monitoring, corrective action, and improvement.

Through this integrated approach, cybersecurity policy compliance becomes an organization-wide governance outcome rather than solely an employee behavioral outcome. The framework provides a conceptual structure that organizations can adapt to their size, risk environment, regulatory obligations, technological infrastructure, and governance requirements. It also establishes a foundation for future empirical research examining the relationships among governance practices, policy implementation, employee compliance, monitoring mechanisms, and organizational cybersecurity outcomes.

Figure 1. Proposed Cybersecurity Governance and Policy Compliance Framework



Source: Author's conceptual framework.

The proposed framework establishes a continuous feedback loop that connects cybersecurity governance with policy compliance and organizational improvement. Governance provides strategic direction and establishes accountability, while cybersecurity policies translate governance expectations into organizational requirements. These requirements are communicated to employees and integrated into organizational processes and practices. Compliance monitoring and assessment are then used to evaluate adherence to established policies and identify potential weaknesses or implementation gaps. Where deficiencies are identified, appropriate corrective actions are implemented to address their underlying causes. Findings from monitoring, corrective actions, incidents, and organizational reviews subsequently inform continuous improvement, governance review, and policy revision, thereby completing the feedback cycle.

The framework is informed by established cybersecurity governance and information security management principles. NIST CSF 2.0 incorporates organizational context, cybersecurity risk management strategy, roles, responsibilities, authorities, policy, and oversight within its Govern function (National Institute of Standards and Technology, 2024). Similarly, ISO/IEC 27001:2022 emphasizes the establishment, implementation, maintenance, and continual improvement of an information security management system (International Organization for Standardization, 2022). COBIT 2019 further contributes governance and management principles for enterprise information and technology, including the evaluation of stakeholder needs, establishment of direction, and monitoring of organizational performance (ISACA, 2019). Although informed by these established approaches, the proposed framework specifically integrates governance responsibilities with the cybersecurity policy-compliance lifecycle to emphasize compliance as a continuous organizational governance process.

VI. DISCUSSION

The proposed Cybersecurity Governance and Policy Compliance Framework emphasizes that effective cybersecurity policy compliance requires more than the development of formal policies, employee awareness, or the implementation of technical security controls. Policy compliance occurs within an organizational environment in which leadership decisions, management practices, employee behavior, technological capabilities, and monitoring processes interact. From this perspective, cybersecurity policy compliance should be understood as a shared organizational responsibility supported by governance rather than solely as an obligation placed on individual employees.

A central implication of the proposed framework is the importance of leadership and accountability in establishing the conditions necessary for effective policy compliance. Organizational leaders establish cybersecurity priorities, assign responsibilities, allocate resources, and determine how cybersecurity risks are incorporated into organizational decision-making. Managers subsequently translate these expectations into operational practices and reinforce policy requirements within their areas of responsibility. Employees remain responsible for following applicable security requirements, but their ability to comply can also depend on whether policies are clearly communicated, appropriate resources are available, and organizational processes support expected security practices. This perspective is consistent with the governance emphasis of NIST CSF 2.0, particularly its attention to organizational context, cybersecurity risk management strategy, roles, responsibilities, policy, and oversight (National Institute of Standards and Technology, 2024).

The framework also contributes to understanding the relationship between organizational governance and employee security behavior. Previous research has demonstrated that information security policy compliance can be influenced by individual, social, and organizational factors, including employee capabilities, social influence, security awareness, self-efficacy, and organizational conditions (Amankwa et al., 2022; Ifinedo, 2014; Siponen et al., 2014). These findings indicate that employee compliance decisions occur within a broader organizational context. Consequently, organizations may benefit from examining the conditions surrounding policy compliance rather than assuming that every instance of noncompliance results exclusively from an employee's unwillingness to follow established requirements.

This distinction has practical implications for the management of policy violations. When noncompliance occurs, organizations should seek to identify its underlying cause before determining an appropriate response. For example, a violation may result from inadequate employee awareness, unclear policy language, insufficient training, technological limitations, competing operational requirements, or inadequate management support. In other circumstances, noncompliance may involve deliberate disregard of established requirements. Differentiating among these causes can support more appropriate corrective actions and help organizations address systemic weaknesses rather than focusing exclusively on individual behavior.

Another important feature of the framework is its emphasis on compliance monitoring as a source of organizational feedback. Monitoring should not be limited to determining whether employees have followed established requirements. It can also provide information about the effectiveness of policies, training programs, technical controls, management practices, and accountability structures. Repeated compliance problems across organizational units, for example, may indicate a broader weakness in policy design or implementation. Monitoring therefore creates an opportunity for organizations to identify patterns, evaluate underlying causes, and make evidence-informed improvements to cybersecurity practices.

Continuous improvement further distinguishes the framework from approaches that treat cybersecurity policy development as a one-time activity. Organizational technologies, cybersecurity threats, regulatory requirements, business processes, and workforce practices continually change. Policies and compliance mechanisms must therefore be periodically reviewed to determine whether they remain appropriate and effective. This principle is consistent with ISO/IEC 27001:2022, which emphasizes the continual improvement of the information security management system (International Organization for Standardization, 2022). Within the

proposed framework, findings from monitoring, audits, incidents, risk assessments, and corrective actions are incorporated into governance review and policy revision, creating a continuous feedback cycle.

The proposed framework also complements existing cybersecurity and information technology governance approaches rather than replacing them. NIST CSF 2.0 provides a broad framework for understanding and managing cybersecurity risk and places greater emphasis on cybersecurity governance through its Govern function (NIST, 2024). ISO/IEC 27001:2022 provides requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISO, 2022). COBIT 2019 provides governance and management objectives designed to support the effective governance and management of enterprise information and technology (ISACA, 2019). The proposed framework builds on principles represented within these established approaches while focusing specifically on the organizational processes connecting governance responsibilities with cybersecurity policy compliance.

From a practical perspective, the framework can provide organizations with a structured way to examine cybersecurity policy compliance across multiple organizational levels. Leadership can use the framework to consider whether appropriate accountability and oversight mechanisms exist; managers can evaluate whether policies are effectively communicated and implemented; cybersecurity personnel can assess monitoring and control mechanisms; and organizations can use identified compliance gaps to inform corrective actions and policy improvements. Because the framework is conceptual, its components can potentially be adapted to organizations of different sizes, industries, technological environments, and cybersecurity maturity levels.

From a theoretical perspective, the framework provides a bridge between behavioral research on information security policy compliance and organizational cybersecurity governance. Behavioral research remains valuable for understanding why employees choose to comply with or violate security requirements (Ifinedo, 2014; Siponen et al., 2014), while governance frameworks establish broader organizational structures for managing cybersecurity and information security risks (ISACA, 2019; ISO, 2022; NIST, 2024). By connecting these perspectives within a continuous policy-compliance lifecycle, the proposed framework conceptualizes compliance as an organizational governance outcome influenced by both individual behavior and organizational conditions.

The framework highlights the interconnected nature of leadership, policy development, communication, implementation, monitoring, corrective action, and continuous improvement. Its principal contribution is the integration of these elements into a continuous governance process in which compliance outcomes generate feedback for future organizational decisions. This approach provides a foundation for organizations seeking to strengthen cybersecurity policy implementation while also creating opportunities for future research to examine how governance mechanisms influence policy compliance and broader cybersecurity outcomes.

VII. CONCLUSION

As organizations become increasingly dependent on digital technologies, cybersecurity governance and policy compliance have become essential components of effective organizational cybersecurity management. Establishing cybersecurity policies and implementing technical controls are necessary, but these measures alone may not ensure effective security practices. Policy effectiveness also depends on clearly defined responsibilities, leadership commitment, effective communication, employee awareness, appropriate implementation mechanisms, systematic monitoring, and organizational processes for addressing identified weaknesses.

This study proposed a Cybersecurity Governance and Policy Compliance Framework that conceptualizes policy compliance as a continuous organizational governance process. The framework integrates leadership and accountability, policy development and alignment, communication and security awareness, policy implementation, compliance monitoring and assessment, corrective action, continuous improvement, governance review, and policy revision within an interconnected feedback cycle. Through this structure, cybersecurity policy compliance extends beyond the development of formal requirements and becomes an ongoing process of implementation, evaluation, organizational learning, and improvement.

The proposed framework is informed by established cybersecurity and information security management approaches, including NIST CSF 2.0, ISO/IEC 27001:2022, and COBIT 2019, as well as research examining information security policy compliance (ISACA, 2019; International Organization for Standardization, 2022; National Institute of Standards and Technology, 2024). Rather than replacing these established approaches, the framework provides a complementary structure that connects governance responsibilities with the practical policy-compliance lifecycle. In doing so, it brings together organizational governance and employee-level compliance considerations within a unified conceptual process.

A central contribution of this study is the recognition that cybersecurity policy compliance should not be understood solely as an employee behavioral outcome. Employees remain responsible for following organizational security requirements; however, compliance also depends on the environment created by organizational leadership and management. Clear policies, adequate resources, relevant training, appropriate technical and administrative controls, consistent oversight, and effective corrective mechanisms can influence

whether security requirements are successfully translated into organizational practice. Policy compliance can therefore be viewed as a shared governance outcome involving leadership, management, cybersecurity personnel, and employees.

The continuous feedback structure of the proposed framework further emphasizes that cybersecurity governance must adapt to changing organizational and risk environments. Findings from compliance monitoring, security incidents, audits, risk assessments, and corrective actions can provide valuable information for governance review and policy revision. Incorporating these findings into subsequent cybersecurity decisions enables organizations to reassess priorities, strengthen controls, clarify responsibilities, and modify policies as technologies, threats, regulatory requirements, and organizational conditions evolve.

From a practical perspective, the proposed framework provides a structured foundation that organizations can use to examine how governance responsibilities are connected to cybersecurity policy implementation and compliance. From a research perspective, it provides a conceptual basis for further investigation of the relationships among leadership, policy management, employee awareness, implementation, monitoring, corrective action, and continuous improvement. Because the framework has not yet been empirically validated, future research should examine its applicability across different industries, organizational sizes, regulatory environments, and cybersecurity maturity levels. Future studies may also develop measurable indicators for its components and evaluate their relationships with policy compliance and broader cybersecurity management outcomes.

Ultimately, strengthening cybersecurity policy compliance requires organizations to move beyond viewing policies as static documents or compliance as an isolated employee responsibility. Cybersecurity policies must operate within a governance system that establishes accountability, supports implementation, evaluates performance, responds to identified weaknesses, and continuously adapts to changing risks. By integrating these activities into a continuous governance cycle, the proposed Cybersecurity Governance and Policy Compliance Framework provides a conceptual foundation for advancing both organizational cybersecurity management and future research on cybersecurity policy compliance.

REFERENCES

- [1]. Alshammari, M. M., & Al-Mamary, Y. H. (2026). Non-technical determinants of information security policy compliance: An integrated PMT-TPB model with psychological ownership, trust, and social influence. *Computers in Human Behavior Reports*, 21, 100947. <https://doi.org/10.1016/j.chbr.2026.100947>
- [2]. Amankwa, E., Looock, M., & Kritzinger, E. (2022). The determinants of an information security policy compliance culture in organisations: The combined effects of organisational and behavioural factors. *Information & Computer Security*, 30(4), 583–614. <https://doi.org/10.1108/ICS-10-2021-0169>
- [3]. Angraini, Alias, R. A., & Okfalisa. (2019). Information security policy compliance: Systematic literature review. *Procedia Computer Science*, 161, 1216–1224. <https://doi.org/10.1016/j.procs.2019.11.235>
- [4]. Balagopal, N., & Mathew, S. K. (2024). Exploring the factors influencing information security policy compliance and violations: A systematic literature review. *Computers & Security*, 147, 104062. <https://doi.org/10.1016/j.cose.2024.104062>
- [5]. Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, 51(1), 69–79. <https://doi.org/10.1016/j.im.2013.10.001>
- [6]. International Organization for Standardization. (2022). ISO/IEC 27001:2022 information security, cybersecurity and privacy protection—Information security management systems—Requirements (3rd ed.). ISO.
- [7]. ISACA. (2018). COBIT 2019 framework: Governance and management objectives. ISACA.
- [8]. Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST Cybersecurity White Paper 29). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.CSWP.29>
- [9]. Quinn, S., Pascoe, C., Barrett, M., Scarfone, K., & Witte, G. (2024). NIST Cybersecurity Framework 2.0: Quick start guide for using the CSF tiers (NIST Special Publication 1302). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.1302>
- [10]. Siponen, M., Mahmood, M. A., & Pahlila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, 51(2), 217–224. <https://doi.org/10.1016/j.im.2013.08.006>