Indonesian Interdisciplinary Journal of Sharia Economics (IIJSE)
e-ISSN: 2621-606X
Vol. 8. No. 2 (2025)
Page: 3349-3367

NIST CYBERSECURITY FRAMEWORK IN THE LENS OF INDONESIAN INTERNAL AUDITORS

Darojatum Muthi'atur Rofi'ah
Universitas Airlangga
darojatum.muthiatur.r-2020@feb.unair.ac.id

Abstract

This study interprets the application of the NIST Cybersecurity Framework (CSF) by Indonesian internal auditors. Employing Paul Ricoeur's hermeneutic phenomenology and Interpretative Phenomenological Analysis (IPA), this research delves into the meaning of CSF from the perspective of internal auditors, including its adaptation to local organizational culture and the factors shaping its effectiveness. Key findings reveal that CSF transcends its role as a technical guide, acting instead as a driver for cybersecurity culture transformation. This study's implications emphasize the necessity of cross-departmental collaboration, context-specific security policy departments, and the enhancement of internal auditor competencies. The novelty of this research lies in its application of in-depth interpretative analysis, showing CSF as an adaptive tool fostering cybersecurity systems attuned to Indonesia's unique characteristics.

Keywords: Internal Audit, Cybersecurity Framework, NIST

INTRODUCTION

Rapid digital transformation has presented organizations in Indonesia with increasingly complex cybersecurity challenges. According to the Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII) report, by 2023, there will be a significant increase in the number of cyberattacks in Indonesia, with more than 1,000 cybersecurity incidents every day. This phenomenon demands a comprehensive cybersecurity framework that can be adapted to the conditions in Indonesia.

Activities that humans once supervised are slowly being transferred to computers. This development has significantly changed the concept of security. Now, the interaction space is not only limited to the physical but extends to cyberspace, which triggers new risks, such as cybercrime and the security of an organization's assets (Sri et al., 2020). The increase in cybercrimes such as ransomware, data theft, and system hacking has encouraged organizations to adopt a more structured approach to cybersecurity. In order to overcome these challenges, a framework is needed to help organizations effectively manage cybersecurity risks.

The Cybersecurity Framework (CSF) was developed by the National Institute of Standards and Technology (NIST) to help organizations manage cybersecurity risks. It was published in 2014 and updated in 2018 (version 1.1) and 2024 (version 2.0) based on various inputs. NIST CSF 2.0 consists of 6 main functions: govern, identify, protect, detect, respond, and recover. The NIST CSF is designed to be flexible and adaptable to different types and sizes of organizations. The framework can also be applied in various stages of organizational maturity, from basic to advanced.

The NIST CSF has emerged as one of the comprehensive frameworks adopted globally, including in Indonesia. Several previous studies have examined the implementation of the NIST CSF in Indonesia; Handoyo & Nigrum (2024) and Amanda et al. (2023) adopted CSF to assess cybersecurity risks in the higher education sector. While in manufacturing companies, CSF is also adopted to monitor the company's information security (Sugara et al., 2019). CSF has collaborated with ISO/IEC 270001:2023 in the government sector to assess information security risks (Putri dkk., 2022). Most of these studies still focus on the technical aspects of implementing the NIST CSF, and research needs to significantly examine the in-

depth understanding of the meaning and interpretation of the framework from the perspective of internal audits in Indonesia.

Internal auditors have an essential role in ensuring the effectiveness of an entity's internal control system, including cybersecurity. They must act independently and objectively in conducting their assessments. Internal auditors manage, evaluate, and improve the company's internal control system. (Ardianto dkk., 2023). Cybersecurity expertise is also needed to provide adequate assurance in today's digitalization era. Internal auditors are responsible for communicating audit findings to management and providing recommendations for improvement.

The role of internal auditors was initially known as a watchdog that focuses on detecting irregularities in an entity (Pramono, 2008). Then, it developed into a strategic business partner due to the birth of the Committee of Sponsoring Organizations of the Treadway Commission (COSO). COSO changes the perspective of internal auditors, which includes three roles: consultant, catalyst, and assurance provider. Now, the role of internal auditors is increasingly complex. We have seen from the adoption of information technology by public sector auditors (Ahmi et al., 2014).

Internal auditors' cybersecurity assurance processes are an integral part of what is needed to deal with increasing cyber threats and protect their digital assets. Internal auditors play a multifaceted role in developing cybersecurity policies and frameworks (Kahyaoglu & Caliyurt, 2018). Ensure compliance (Stafford et al., 2018) and mitigate risks related to cyber incidents (Darmawati, 2022)

Analysis of the literature reveals a research gap in understanding the implementation of the NIST CSF from the perspective of internal auditors in Indonesia. Existing studies have yet to comprehensively explore the interpretation and contextualization of this framework using Paul Ricoeur's hermeneutic phenomenological approach. This approach enables an in-depth understanding of layers of meaning through interpretation of the NIST CSF 2.0 text and practitioners' experiences based on a literature study of the adoption of the NIST CSF in previous research.

This research will explore how internal auditors in previous studies interpret NIST CSFs in their professional practice in Indonesia and identify challenges and

recommendations to improve the effectiveness of the role of internal auditors in supporting cybersecurity in Indonesia. This means that researchers consider factors specific to Indonesia, such as regulations, culture, and cybersecurity maturity level.

The main contribution of this research is to bridge the gap between international standards and local practices and provide a theoretical foundation for developing a more contextualized cybersecurity audit methodology. By collaborating Paul Ricoeur's hermeneutic phenomenology method with the Interpretative Phenomenological Analysis (IPA) method, this research produces not only empirical data on the implementation of the NIST CSF but also an in-depth understanding of internal auditors' interaction with international standards in the Indonesian socio-cultural context.

REVIEW OF LITERATURE

Cybersecurity Framework

The NIST Cybersecurity Framework (CSF) is a comprehensive framework that has been adopted globally to manage cybersecurity risks. It consists of 3 main components: Core, Organizational Profiles, and Tiers (NIST, 2018). The framework offers a flexible risk-based approach and can be integrated with existing risk management systems or build new cybersecurity programs. The NIST CSF has been widely recognized by the public and private sectors globally as a reference framework (AWS, 2016).

The NIST CSF introduces a framework structure consisting of 6 key functions in cybersecurity risk management. The govern function, a recent addition to version 2.0, focuses on governance and the integration of cybersecurity into an Enterprise Risk Management (ERM) strategy. The other five functions include identify (identifying business and resources), protect (security protection), detect (detecting cyber incidents), respond (handling cyber incidents), and recover (service recovery). The following is an image of the CSF 2.0 functions:

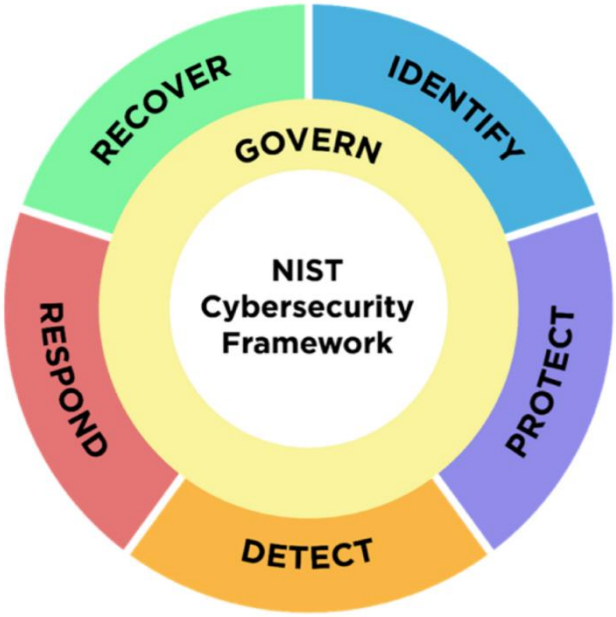

Figure 1
Cybersecurity Framework 2.0 (NIST, 2024)

Each NIST CSF function is represented with a verb that reflects its primary purpose and is organized in a hierarchical structure consisting of categories and subcategories. Categories group the cybersecurity outcomes that make up the function, while subcategories detail specific technical and management activities.

There are integral components that cannot be separated in this framework, namely Profiles and Tiers. Profiles serve as measurement instruments that enable comparisons between actual conditions and target profiles in cybersecurity practices. Meanwhile, Tiers provide assessment metrics with a spectrum of 4 maturity levels, ranging from Partial to Adaptive, which measure the sophistication of risk management practices and governance of cybersecurity structures.

The NIST CSF is a framework developed to improve cybersecurity risk management in critical infrastructure. In Indonesia, the role of internal auditors is increasingly important as cyber risks increase, especially after the pandemic that has driven massive digitization. Based on PwC (2014), the NIST CSF framework needs to be a foolproof formula for cybersecurity. The benefits will be noticed by those who need to pay more attention to the implementation of the guidelines. This is because the framework contains leading practices

from various standards bodies that have been proven to work and can provide policy advantages to organizations that adopt them.

In the context of this research, this framework is an important object of analysis to understand how internal auditors in Indonesia interpret, adapt, and implement these international standards in the local context, given their strategic role in strengthening the cybersecurity governance of an organization.

Internal Audit

An internal audit is a professional and independent evaluation mechanism that plays a vital role in controlling and improving an entity's operations. IIA (2013) defines internal audit as an independent and objective assurance and consulting activity designed to provide added value and optimize organizational operations. Soemarso (2005) expanded this definition by emphasizing the evaluation of the effectiveness of internal control and the provision of recommendations for improvement.

Post-2000, digital transformation has changed the internal audit landscape. Sawyer (2003) identified the urgency of competency in information systems auditing, while Pickett (2015) emphasized the importance of cross-jurisdictional understanding in multinationals. This transformation reflects how globalization and developments in information technology have driven the expansion of the scope and complexity of the internal audit practice, requiring auditors to develop new competencies to meet the challenges of the digital age.

In general, internal auditors play a vital role in achieving organizational goals, especially in the era of digital transformation that creates new dimensions in audit practices. Referring to research by Alina et al. (2017) on the five crucial steps of internal audit's role in cybersecurity in line with NIST's CSFs, namely protect, detect, business continuity, react, and improve. Pundmann et al. (2017) reinforced this argument by underscoring the significance of cyber threats to business continuity, which requires internal auditors to take a strategic position in cybersecurity risk evaluation.

The significant challenges internal auditors face is not only limited to conventional audit competencies but include the need to master Information Technology (IT)(Sri et al., 2020). This is evidenced by the tendency of large organizations to prefer using the services of auditors with IT capabilities, given the strategic role of IT in various aspects of the

organization, from budget planning to accountability. In this context, internal auditors contribute to effective corporate governance through a broad spectrum of assurance and advisory services (Risfa & Lestari, 2023).

RESEARCH METHOD

This research uses a qualitative approach with the hermeneutic phenomenology method developed by Paul Ricoeur. This methodology was chosen because it reveals the deep meaning of previous literature regarding adopting the NIST CSF in Indonesia. Ricoeur and Thompson (2016) offer a unique approach by integrating phenomenology and hermeneutics. In this approach, text is seen as a discourse. That is fixed in writing and allows it to be interpreted independently of the author's intentions.

In the context of phenomenology, this research seeks to explore the perspective of internal auditors as reflected in previous literature on adopting the NIST CSF in Indonesia. The phenomenological approach allows researchers to "bracket" or confine personal assumptions to reveal the pure experience of internal auditors in implementing the framework. Meanwhile, the hermeneutic dimension helps understand how cultural, social, and organizational contexts influence auditors' interpretations of the NIST CSF.

Data collection was conducted through a systematic literature study of scientific articles that discuss the implementation of the NIST CSF in the context of internal auditing in Indonesia. The stages of analysis in this research incorporate the hermeneutic circle of Ricoeur and Thompson (2016) and the Interpretative Phenomenological analysis (IPA) method which consists of:

1. Prefiguration

   Through in-depth reading of the literature related to the NIST CSF in Indonesia. At this stage, the researcher built an initial understanding of the context and general meaning of the NIST CSF. Focus on basic patterns and naive meanings that emerge.

2. Theme Identification (Configuration or Structural Reasoning)

   After a thorough reading, the researcher identified critical themes in the literature. When conducting structural analysis, researchers will look for patterns or themes related to the adoption of the NIST CSF in Indonesia by internal audits. The themes identified may

include technical barriers, cultural aspects, or regulations that affect the implementation of the NIST CSF. To ensure that the interpretations reflect the data, the researcher performs "bracketing" or confinement of personal assumptions to ensure that the interpretations remain neutral and unbiased.

3. Theme Clustering and In-Depth Analysis (Refiguration)

   The themes that have been identified are then grouped and analyzed in depth using the concept of hermeneutic circles. This involved interpreting how internal auditors interpret and implement the NIST CSF in Indonesia. The researcher used Ricoeur's concept of the hermeneutic circle, involving iterative interpretation, to explore the hidden meaning in the text.

4. Deep Interpretation (Appropriation)

   Ricoeur and Thompson (2016) describe appropriation as 'repossessing' a previously unfamiliar understanding and internalizing it in the research context. At this stage, interpretation continues beyond theoretical understanding but also at how that understanding can be applied in the wider context of the field. The researcher connects the analysis results with broader theory and practice and explores how the NIST CSF is adapted to Indonesian culture and organizational structure.

5. Synthesis and Conclusion

   After all stages of interpretation are completed, all findings are synthesized to form a comprehensive understanding of the factors influencing the implementation of the NIST CSF in Indonesia. The new meanings generated from this interpretation can enrich the understanding of the auditor's role in implementing the NIST CSF in Indonesia.

Through this procedure, the researcher systematically uncovered how internal auditors in Indonesia interpret the NIST CSFs. The interpretation process is iterative, allowing the researcher to continue to refine understanding as the data is explored more deeply. According to Ricoeur and Thompson (2016), the hermeneutic process is an endless circle that evolves understanding as perspectives change. Therefore, it is necessary to return to the data repeatedly to strengthen the interpretation or find aspects that may have been missed.

RESULTS AND DISCUSSION

Prefiguration

Initial understanding and interpretation aim to obtain a lay and concise overview of the context of NIST CSF adoption in Indonesia. Through iterative reading with adequate time intervals, researchers can develop new perspectives without bias from previous research. Based on the analysis of 10 articles examining the implementation of the NIST CSF in Indonesia, various interpretations were identified in internal auditors' understanding of the framework.

The naive meaning that emerges from this initial understanding shows that internal auditors across sectors interpret the NIST CSF as a strategic instrument for identifying and managing cybersecurity risks. This finding is supported by various empirical studies, such as research by Hidayat & Wang (2023) which shows the central role of the NIST CSF in evaluating the effectiveness of cybersecurity operations in the non-bank financial sector. In addition, Putro et al. (2024) highlighted the importance of the NIST CSF in protecting critical infrastructure through a sustainable approach. The cyclical and proactive nature of the NIST CSF allows it to continuously adapt to the dynamic threat landscape, making it a relevant framework for organizations in Indonesia.

As for its implementation in Indonesia, there are several obstacles, including technical limitations, regulations, and organizational cultural awareness. The main obstacles are technical challenges such as system complexity and the need to adjust to regulations in Indonesia. Research by Sama et al. (2021) supports this finding. In addition, the lack of infrastructure readiness is also a hindering factor, especially in the 'identify' function that has yet to cover all controls in the manufacturing sector (Sugara et al., 2019). In the education sector, Handoyo & Nigrum (2024) showed that the need for more documentation and technical control is an obstacle to implementing the NIST CSF.

Internal auditors utilize the NIST CSF to evaluate and improve cybersecurity maturity. The framework helps identify security gaps and align security efforts with business objectives, especially in the sensitive insurance sector (Hidayat & Wang, 2023). However, the implementation of the NIST CSF in Indonesia faces challenges, including a need for more awareness about the importance of cybersecurity (Amanda et al., 2023). At the same time,

Balafif (2023) showed that MSMEs still view cybersecurity as an additional cost rather than an investment. This hinders the effectiveness of risk identification, and applying the NIST CSF is considered less of a priority. Therefore, it is necessary to increase cybersecurity awareness by the conditions and structure of the organization.

The success of CSF implementation in Indonesia is also highly dependent on its ability to adapt to Indonesian culture and regulations. Retnowardhani et al. (2019) exemplified how the implementation of CSF on BYOD systems in the manufacturing sector requires special consideration of work practices and organizational culture. In addition, cross-departmental collaboration is important in maintaining cybersecurity, not just the IT team (Tan and Soewito, 2022). Thus, CSF can catalyze building an inclusive and sustainable cybersecurity culture.

This framework is not only a technical instrument but also a catalyst in transforming organizational culture. Applying the NIST CSF at BPS West Kalimantan allows the organization to adapt to the evolving cyber threat landscape (Putri et al., 2022). The adoption of the NIST CSF in Indonesia ideally needs to be tailored to each organization's unique cultural and business context. This will create a strong foundation for a proactive and sustainable cybersecurity culture. It is important to remember that the NIST CSF is not just a list of technical controls, but a holistic framework that considers the overall context of the organization.

Theme Identification (Configuration)

Based on the structural analysis of the NIST CSF implementation in various sectors in Indonesia reveals several key themes that are interrelated and affect the successful adoption of the framework. Among them are:

1. Framework Adaptation to Cultural Context and Organizational Structure

   Several articles highlighted the importance of internal auditors in Indonesia adapting the NIST CSF to the existing organizational culture. Amanda et al. found that stakeholder involvement is crucial, especially in risk management. Meanwhile, increasing cybersecurity awareness at all levels of the organization is an important prerequisite for dealing with increasingly complex cyber threats. Hidayat and Wang (2023); Balafif (2023). Implementing the NIST CSF requires a change in organizational culture so that

all stakeholders participate in maintaining cybersecurity. (Tan & Soewito, 2022). Indonesia's hierarchical organizational culture will slow down the adoption process because it requires approval from various levels of management.

2. Technical Constraints and Infrastructure Readiness

   The implementation of the NIST CSF in Indonesia faces significant obstacles related to infrastructure and technology. Sama et al. and Sugara et al. identified limitations in existing infrastructure, such as inadequate documentation systems. The existence of legacy systems and outdated hardware or software makes it difficult to manage security risks and updates promptly. (Hidayat & Wang, 2023). Therefore, technology modernization is imperative to support optimal CSF implementation.

3. Regulatory Limitations and Policy Adjustments

   Regulatory limitations that have yet to fully support the integration of the NIST CSF with security standards in Indonesia were also identified as obstacles. Implementing the NIST CSF is also limited by regulations that have yet to be fully adapted to globally applicable standards. Sama et al. and Putro et al. (2024) highlighted that national policies often need to accommodate the cybersecurity aspects covered in the NIST CSF comprehensively. This necessitates adjusting local policies to align with global cybersecurity practices.

4. Limited Human Resources and Security Awareness

   Limited employee competence in cybersecurity standards slows down the implementation of the framework as a whole (Putri et al., 2022). This lack of competency hampers the overall effectiveness of the NIST CSF implementation. Therefore, training and human resource development investment are crucial to increasing cybersecurity awareness and technical capacity.

5. Internal Auditors' Role as Risk Assessors, Consultants and Cybersecurity Facilitators

   There are indications of a shift in the role of internal auditors from a traditional approach to a cyber risk-based approach. In Hidayat & Wang (2023), internal auditors evaluate cybersecurity maturity levels and help align cybersecurity objectives with business needs. With a focus on continuous monitoring, internal auditors ensure the organization can detect changes or threats in real-time, as discussed in the study of Putri et al. (2022).

In addition, auditors encourage cross-departmental collaboration to ensure compliance with security protocols (Tan & Soewito, 2022). Thus, internal auditors are critical actors in Indonesia's cybersecurity transformation.

6. The Impact of Transformation on Cybersecurity Practices

   Implementing the NIST CSF has significantly transformed cybersecurity practices across sectors. Implementing the framework in government has led to more structured information security governance improvements (Sensuse et al., 2022). In the manufacturing sector, the CSF encourages organizational culture transformation toward higher cybersecurity awareness, such as using personal devices (BYOD)(Retnowardhani et al., 2019). Furthermore, the shifting role of internal auditors in implementing the NIST CSF catalyzes change within organizations, encouraging more collaborative and awareness-based security practices.

Through these themes, the adaptation of the NIST CSF in Indonesia faces various complex challenges involving technical aspects, culture, strengthening regulations, developing human resources, and the active role of internal auditors. The successful implementation of the NIST CSF is highly dependent on the organization's ability to adapt to this framework in the local context.

Deep Analysis (Refiguration)

This stage of refiguration analysis grouped the themes from the configure analysis into main categories to explore deeper meanings. In-depth analysis uses Ricoeur's hermeneutic circle approach, which connects initial interpretation and reinterpretation through a cyclic process in the practice of internal auditors. The following is a grouping of themes and interpretations:

1. Adaptation of Organizational Culture and Structure

   Implementing the NIST CSF in Indonesia requires adapting to the organizational culture and hierarchical structure. Tan & Soewito (2022) showed that implementing the NIST CSF in education required organizational culture and hierarchical structure adjustments. Internal auditors began to interpret the CSF as more than a technical guide, but rather a tool to instill cybersecurity awareness at all levels of the organization. Through this

adaptation, auditors understand that cybersecurity is an integral part of the culture that must be implemented together, not just the IT team.

2. Obstacles in Implementing the NIST CSF

   NIST's CSF faces limited technical constraints, policy adjustments, and a need for more competent human resources in cybersecurity. Legacy infrastructure and limited documentation systems hindered the implementation (Sugara et al., 2019). Internal auditors interpret these constraints as a need to modernize Indonesia's cybersecurity infrastructure. Policies in Indonesia are often outside the CSF standard, so interpretation is needed by the Indonesian legal and regulatory context (Sama et al., 2021) ; (Putro et al., 2024). Employees who need an understanding of cybersecurity help the effectiveness of CSF implementation (Putri et al., 2022). Internal auditors also see this framework as supporting ongoing training and education programs. The effect is that understanding cybersecurity's importance is more evenly distributed.

3. Internal Auditor's Role in Cybersecurity

   The CSF shifts the role of internal auditors from mere risk evaluators to active security consultants, helping organizations implement cybersecurity best practices. Auditors play an active role in assessing and aligning cybersecurity needs with business objectives (Hidayat & Wang, 2023). This framework guides internal auditors to design proactive strategies aligned with business objectives and the development of cyber threats in Indonesia.

4. Impact of Cybersecurity Practice Transformation

   Adopting the NIST CSF is driving significant changes in cybersecurity practices in various sectors in Indonesia. CSF implementation helps organizations create more structured and threat-responsive security governance (Putro dkk., 2024). This framework is a catalyst that integrates cybersecurity auditing into organizational governance. Thus, internal auditors interpret the CSF as a foundation for adaptively strengthening organizational security.

Using Ricoeur's hermeneutic circle approach, internal auditors in Indonesia see the NIST CSF as a transformational tool, not just a technical instrument. Technical and cultural adjustments, people development, and aligned policies influence the successful

implementation of the CSF. The CSF is a compliance guide and the basis for building adaptive cybersecurity resilience in various sectors in Indonesia. An in-depth analysis of the literature found that internal auditors in Indonesia often interpret the NIST CSF as a prescriptive framework. However, in practice, they make significant adjustments.

Hidden Meaning (Appropriation)

Based on Ricoeur's hermeneutic circle approach, the researcher delves deeper into how internal auditors in Indonesia's understanding of the NIST CSF has evolved into a framework that is more than just a technical guide. At this appropriation stage, interpretations from the previous analysis are internalized into Indonesian culture and organizational structure. This appropriation deepens the openness between the CSF and the fundamental dynamics in the field.

1. NIST CSF as a Transformational Tool in Indonesia

   The NIST CSF in Indonesia does not stop at technical implementation but becomes a transformation process that permeates the organizational structure and work culture. CSF, as a tool, can shape organizational culture through a collective understanding of the importance of cybersecurity. The example raised by Putro et al.(2024) shows that the framework drives a more profound change-enhancing adaptive security governance structure amidst dynamic cyber threats. Theoretically, this aligns with organizational change theory (Force Field Theory). Frameworks such as CSF act as change agents that shape new organizational practices. The need for organizational openness to change (Eysenck & Lewin, 1952), so that CSF is not only seen as an obligation but as an important foundation in the creation of responsive and proactive security.

2. Cultural Relevance and Adaptation in Cybersecurity Practice

   Adapting the NIST CSF requires cultural adjustments and a collaborative approach in the Indonesian context, which has a distinctive hierarchical structure. A global framework such as CSF can only be applied directly by integrating local culture. Therefore, in its application, it is necessary to internalize cybersecurity values adapted to local norms to be more effective. Internal auditors can encourage a common understanding at various levels of the organization with training that is not only technical but also includes the socialization of cybersecurity values that are readily accepted. The

CSF becomes more meaningful when socialized as a collective responsibility, not just an additional obligation.

3. Transformation of the Internal Auditor's Role

   Internal auditors in Indonesia are more than just watchdogs; they are facilitators who drive change to a more structured and adaptive cybersecurity culture. By implementing the NIST CSF, internal auditors assess risk and serve as change consultants, helping organizations identify specific needs and providing appropriate implementation guidance. Within the framework of the Leading Change Theory by Kotter (2007), the role of internal auditors in the study of Hidayat & Wang (2023) reflects their role as change agents who guide organizations in navigating cybersecurity challenges. Internal auditors reinforce long-term and sustainable cybersecurity strategies, supporting organizations to build resilience and rapid response to dynamic threats.

4. CSF's Contribution to the Formation of a Collective and Dynamic Understanding of Security

   The interpretation of the CSF as a means for the dynamic enhancement of collective understanding of cybersecurity becomes the central point of appropriation. This framework, as Putro et al. understood, increases awareness of evolving cyber threats, and builds human resource capacity in the face of a changing risk landscape. The CSF is a foundation for continuous monitoring, allowing organizations to remain responsive to changing risks with evolving collective understanding. This emphasizes that the success of the CSF relies on the organization's ability to continuously learn and adapt, where a dynamic understanding of security allows internal auditors and the organization to respond to rapidly changing threats.

Implementing CSF in Indonesia creates synergy between global standards and the local context, becoming more than a technical guideline. It also reflects an organization's need to build cybersecurity resilience that fits Indonesia's culture and social structure. Internal auditors serve as change leaders in implementing this understanding in the field, encouraging organizations to apply the CSF as a collective and dynamic effort to maintain cybersecurity.

Based on the four stages of analysis above, the findings of this study show that the implementation of the NIST CSF in Indonesia faces various factors that affect its success—starting from cultural adaptation and technical challenges to the increasingly complex role of internal auditors. In the early stages, the NIST CSF was understood as a strategic framework for identifying and managing cybersecurity risks. However, a deeper interpretation of the results shows that the NIST CSF also functions as a transformational instrument that supports establishing a responsive and collective cybersecurity culture in the organization.

In Indonesia's hierarchical organizational culture, the NIST CSF requires adaptation to local norms to maximize its effectiveness. Internal auditors act as facilitators of change, helping to create collective awareness at all levels of the organization and supporting more inclusive and collaborative cybersecurity implementation. This role reflects a shift from risk oversight to change agent, integrating cybersecurity strategies into the organization's daily processes and practices.

The new meanings generated from this analysis enrich the understanding of the role of internal auditors in implementing the NIST CSF in Indonesia. Internal auditors now not only perform technical functions but also play a role in building sustainable cybersecurity resilience through an adaptive and dynamic approach. Thus, implementing the NIST CSF in Indonesia not only fulfills compliance but also forms the foundation of cybersecurity, which is holistic and relevant to the social and cultural context of organizations in Indonesia.

CONCLUSION

This research reveals that implementing the NIST CSF in Indonesia involves cultural adaptation, technical challenges, and a more complex role for internal auditors. The NIST CSF not only serves as a technical guide but also drives transformation within the organization. Internal auditors act as change agents to build a responsive, collaborative cybersecurity culture. This study highlights the new meaning that internal auditors oversee risk and facilitate security resilience through an adaptive approach.

The theoretical contribution of this research is related to the adoption of global standards in the local context (Indonesia), as well as practical value in the form of guidance

for developing internal auditor competencies in the digital era. The limitations of this research include the need for primary data from interviews or direct observation, but in-depth literature analysis still provides valuable insights into Ricoeur's hermeneutic phenomenology approach.

Practical recommendations for internal auditors include strengthening security culture through values-based education, adaptive training development, cross-departmental collaboration, and continuous monitoring. Further research is recommended to explore internal audit's role in cybersecurity across various sectors in Indonesia and its impact on overall cybersecurity effectiveness.

REFERENCES

Ahmi, A., Saidin, S. Z., & Abdullah, A. (2014). IT Adoption by Internal Auditors in Public Sector: A Conceptual Study. *Procedia - Social and Behavioral Sciences*, *164*. https://doi.org/10.1016/j.sbspro.2014.11.151

Amanda, D., Mutiah, N., & Rahmayudha, S. (2023). Analisis Tingkat Kematangan Keamanan Informasi Menggunakan NIST Cybersecurity Framework dan CMMI. *Coding Jurnal Komputer dan Aplikasi*, *11*(2). https://doi.org/10.26418/coding.v11i2.65088

Ardianto, A., Anridho, N., Ngelo, A. A., Ekasari, W. F., & Haider, I. (2023). Internal audit function and investment efficiency: Evidence from public companies in Indonesia. *Cogent Business and Management*, *10*(2). https://doi.org/10.1080/23311975.2023.2242174

Balafif, S. (2023). Penyesuaian Model Ketahanan Siber Umkm Di Indonesia Dengan Nist Cybersecurity Framework. *Jurnal Informatika: Jurnal Pengembangan IT*, *8*(3). https://doi.org/10.30591/jpit.v8i3.5662

Bozkus Kahyaoglu, S., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal*, *33*(4). https://doi.org/10.1108/MAJ-02-2018-1804

Handoyo, E., & Izza Eka Nigrum. (2024). Penilaian risiko keamanan siber kampus menggunakan framework cybersecurity NIST 1.1. *Jurnal CoSciTech (Computer Science and Information Technology)*, *4*(3). https://doi.org/10.37859/coscitech.v4i3.5628

Hidayat, V. K., & Wang, G. (2023). A Comprehensive Cybersecurity Maturity Study for Nonbank Financial Institution. *Journal of System and Management Sciences*, *13*(5). https://doi.org/10.33168/JSMS.2023.0534

Kotter, J. P. (2007). Leading change: Why transformation efforts fail. Dalam *Harvard Business Review* (Vol. 85, Nomor 1). https://doi.org/10.1007/978-1-137-16511-4_7

Kunaifi, A., Ali Sad, A., & Mawardi, A. (2023). Opportunities Analysis of Indonesian Sharia Bank (BSI) Become Top 5 Bank in Indonesia Based on Asset Strength and Vision Mission. *Majapahit Journal of Islamic Finance and Management*, *2*(1), 1–22. https://doi.org/10.31538/mjifm.v2i1.21

Maria Alina, C., Elena Cerasela, S., & Gabriela, G. (2017). Internal Audit Role in Cybersecurity. *Economic Sciences Series*, *17*(2).

National Institute of Standards and Technology. (2023). *NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework Note to Reviewers*. U.S. Department of Commerce.

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity [v1.1 Draft]. *National Institute of Standards and Technology*.

Pramono, S. E. (2008). Transformasi Peran Internal Auditor dan Pengaruhnya Bagi Organisasi. *Media Riset Akuntansi, Auditing & Informasi*, *3*(2). https://doi.org/10.25105/mraai.v3i2.2820

Pundmann, S., Juergens, M., Young, C., Kovesdy, G., & Wilson, G. (2017). Cybersecurity and the role of internal audit - An urgent call to action. *An urgent call to action*.

Putri, T. S., Mutiah, N. M., & Prawira, D. P. (2022). ANALISIS MANAJEMEN RISIKO KEAMANAN INFORMASI MENGGUNAKAN NIST CYBERSECURITY FRAMEWORK DAN ISO/IEC 27001:2013 (Studi Kasus: Badan Pusat Statistik Kalimantan Barat). *Coding Jurnal Komputer dan Aplikasi*, *10*(02). https://doi.org/10.26418/coding.v10i02.54972

Putro, P. A. W., Sensuse, D. I., & Wibowo, W. S. S. (2024). Framework for critical information infrastructure protection in smart government: a case study in Indonesia. *Information and Computer Security*, *32*(1). https://doi.org/10.1108/ICS-03-2023-0031

PwC. (2014). Why you should adopt the NIST cybersecurity framework. *PwC*, *May*.

Retnowardhani, A., Diputra, R. H., & Triana, Y. S. (2019). Security risk analysis of bring your own device (BYOD) system in manufacturing company at Tangerang. *Telkomnika (Telecommunication Computing Electronics and Control)*, *17*(2). https://doi.org/10.12928/TELKOMNIKA.v17i2.10165

Ricoeur, P., & Thompson, J. B. (2016). Hermeneutics and the human sciences: Essays on language, action and interpretation. Dalam *Hermeneutics and the Human Sciences: Essays on Language, Action and Interpretation*. https://doi.org/10.1017/CBO9781316534984

Risfa, M., & Lestari, W. (2023). Metamorfosis Peran Auditor Internal. *Owner*, *7*(3). https://doi.org/10.33395/owner.v7i3.1528

Sama, H., Licen, L., Saragi, J. S. D., Erline, M., Kelvin, K., Hartanto, Y., Winata, J., & Devalia, M. (2021). STUDI KOMPARASI FRAMEWORK NIST DAN ISO 27001 SEBAGAI STANDAR AUDIT DENGAN METODE DESKRIPTIF STUDI PUSTAKA. *Rabit: Jurnal Teknologi dan Sistem Informasi Univrab*, *6*(2). https://doi.org/10.36341/rabit.v6i2.1752

Sawyer, L. B. (2003). Sawyer's Internal Auditing: The Practice of Modern Internal Auditing. *The Institute of Internal Auditors*.

Sensuse, D. I., Putro, P. A. W., Rachmawati, R., & Sunindyo, W. D. (2022). Initial Cybersecurity Framework in the New Capital City of Indonesia: Factors, Objectives, and Technology. Dalam *Information (Switzerland)* (Vol. 13, Nomor 12). https://doi.org/10.3390/info13120580

Sherina Darmawati, D. (2022). Pengaruh Auditor Internal dan Kebijakan Manajeman Terhadap Efektivitas Keamanan Siber. *Jurnal Ekonomi Trisakti*, *2*(2).

Soemarso, S. R. (2005). Akuntansi suatu pengantar, edisi kelima. *Jakarta: Salemba Empat*, *5*.

Spencer Pickett, K. H. (2015). The internal auditing handbook: Third edition. Dalam *The Internal Auditing Handbook: Third Edition*. https://doi.org/10.1002/9781119201717

Sri, D. J., Perwakilan, P., Provinsi, B., & Selatan, S. (t.t.). *Auditor Internal Pemerintah di Era Dgital*.

Stafford, T., Deitz, G., & Li, Y. (2018). The role of internal audit and user training in information security policy compliance. *Managerial Auditing Journal*, *33*(4). https://doi.org/10.1108/MAJ-07-2017-1596

Sugara, V. I., Syahrial, H., & Syafrullah, M. (2019). Sistem Pemeriksaan Keamanan Informasi Menggunakan National Institute of Standards and Technology (NIST) Cybersecurity Framework. *Komputasi: Jurnal Ilmiah Ilmu Komputer dan Matematika*, *16*(1). https://doi.org/10.33751/komputasi.v16i1.1591

Tan, T., & Soewito, B. (2022). Manajemen Risiko Serangan Siber Menggunakan Framework NIST Cybersecurity di Universitas ZXC. *Journal of Information System, Applied, Management, Accounting and Research*, *6*(2).

The Institute of Internal Auditors (IIA). (2013). The IIA's Global Internal Audit Competency. *IIA*.