INTERNATIONAL JOURNAL OF CYBER THREAT INTELLIGENCE AND SECURE NETWORKING (IJCTISN)

eISSN: 3087-4297

Volume. 03, Issue. 01, pp. 06-12, January 2026"

Strategic Risk-Based Cybersecurity Governance: Integrating Policy Frameworks, Organizational Controls, and Compliance Mechanisms for Contemporary Information Systems

Dr. Nyra Quellin
Department of Information Systems, University of Pretoria, South Africa

Article Received: 05/11/2025, Article Revised: 25/11/2025, Article Accepted: 20/12/2025, Article Published: 21/01/2026

ABSTRACT

The rapid intensification of digital transformation across public and private sectors has elevated cybersecurity governance from a technical concern to a core strategic and policy-driven imperative. Contemporary organizations operate within increasingly complex threat environments characterized by ransomware proliferation, insider risks, regulatory fragmentation, and systemic interdependencies across information infrastructures. As a result, traditional compliance-oriented cybersecurity approaches have proven insufficient to address evolving socio-technical risks. This research article develops a comprehensive, publication-ready theoretical and analytical examination of strategic cybersecurity governance through a risk-based policy lens. Grounded strictly in the provided scholarly and practitioner-oriented references, the study synthesizes governance frameworks, organizational theory, and compliance research to construct an integrated understanding of how cybersecurity can be governed effectively at the enterprise and board levels.

Central to the analysis is the conceptualization of cybersecurity governance as an adaptive, risk-informed, and strategically embedded process rather than a static set of controls. Building upon contemporary governance literature and policy-oriented cybersecurity frameworks, the article critically examines how risk-based approaches align cybersecurity strategy with organizational objectives, regulatory expectations, and evolving threat landscapes. Particular emphasis is placed on the role of strategic policy frameworks that translate technical security requirements into governance mechanisms capable of guiding decision-making, accountability, and resource allocation across organizational hierarchies (Mohammed Nayeem, 2025).

The study adopts a qualitative, interpretive methodology grounded in structured literature analysis and comparative framework examination. Rather than empirical measurement, the research emphasizes deep theoretical elaboration, historical contextualization, and critical synthesis of governance models such as NIST, COBIT, ISO/IEC 27001, and CIS Controls. The results highlight recurring governance challenges, including misalignment between boards and technical teams, overreliance on compliance checklists, and insufficient integration of risk intelligence into policy formulation. The discussion advances scholarly debate by positioning strategic cybersecurity governance as a form of enterprise risk governance that requires continuous learning, cross-functional coordination, and policy agility.

By contributing an integrative theoretical narrative, this article addresses a significant literature gap concerning the strategic operationalization of risk-based cybersecurity governance. It offers nuanced implications for researchers, policymakers, and organizational leaders seeking to move beyond reactive security postures toward resilient, governance-driven cybersecurity ecosystems.

KEYWORDS

Cybersecurity governance; risk-based policy; IT compliance; enterprise risk management; information security governance; strategic IT governance.

INTRODUCTION

The contemporary digital environment is defined by pervasive connectivity, accelerated innovation, and an

unprecedented reliance on information systems to sustain organizational operations, economic activity, and social interaction. Within this environment, cybersecurity has emerged as a foundational concern not only for technical specialists but also for organizational leaders, policymakers, and regulatory authorities. The increasing frequency and sophistication of cyber incidents, ranging from ransomware attacks to systemic data breaches, has exposed fundamental weaknesses in how organizations conceptualize and govern cybersecurity risk (Alejandro, Guarda, & Ninahualpa Quiña, 2019). These developments have catalyzed a shift in scholarly and practitioner discourse from narrow technical defenses toward broader questions of governance, accountability, and strategic oversight (Swinton & Hedges, 2019).

Cybersecurity governance, as a concept, extends beyond the implementation of security technologies or compliance with prescribed standards. It encompasses the structures, processes, and relational mechanisms through which organizations direct and control cybersecurity activities in alignment with strategic objectives and risk appetites (De Haes et al., 2019). Historically, information security was often relegated to operational or technical domains, managed by IT departments with limited board-level engagement. However, as cyber risks have demonstrated the capacity to disrupt organizational survival, reputation, and regulatory standing, cybersecurity governance has increasingly become a board-level responsibility (Al-sartawi, 2020). This evolution reflects a broader recognition that cybersecurity is inseparable from enterprise risk management and organizational resilience.

Despite this recognition, significant gaps persist between governance aspirations and operational realities. Many organizations continue to adopt compliance-driven cybersecurity models that prioritize adherence to standards and regulations over dynamic risk assessment and strategic integration (DataGuard, 2018). While frameworks such as ISO/IEC 27001 and the NIST Cybersecurity Framework provide valuable guidance, their effectiveness depends on how they are interpreted, contextualized, and embedded within organizational governance structures (Edward, 2016; Calder, 2018). The literature increasingly suggests that a purely control-based or checklist-oriented approach may create an illusion of security while failing to address emerging threats and organizational vulnerabilities (Cram, D'Arcy, & Proudfoot, 2019).

Risk-based cybersecurity governance has therefore gained prominence as a paradigm that emphasizes prioritization, adaptability, and strategic alignment. Rather than treating all security controls as equally important, risk-based approaches focus on identifying, assessing, and managing risks in accordance with their potential impact and likelihood (Federal Virtual Training Environment, 2020). This perspective aligns cybersecurity decision-making with organizational objectives, enabling leaders to allocate resources more effectively and to justify security investments in strategic terms. Importantly, risk-based governance also facilitates communication between technical experts and non-technical decision-makers by framing cybersecurity in the language of risk and value (Mohammed Nayeem, 2025).

The theoretical foundations of risk-based governance draw from enterprise governance of IT, organizational control theory, and risk management scholarship. COBIT, for example, explicitly positions IT governance as an integral component of enterprise governance, emphasizing value creation, risk optimization, and resource management (De Haes et al., 2019). Similarly, the NIST Cybersecurity Framework encourages organizations to assess their current and target security postures based on risk tolerance and business context rather than universal benchmarks (Calder, 2018). These frameworks reflect a broader governance trend toward contextualization and strategic flexibility.

However, the adoption of risk-based cybersecurity governance is not without challenges. Empirical studies have documented persistent gaps in policy compliance, often influenced by human behavior, organizational culture, and competing priorities (Cram et al., 2019). Moreover, boards and senior executives may lack the technical literacy required to meaningfully engage with cybersecurity risk, leading to overreliance on symbolic governance mechanisms or delegated responsibility (Al-sartawi, 2020). These issues underscore the need for governance models that integrate technical expertise, organizational learning, and policy coherence.

The literature further highlights the growing interdependence between cybersecurity governance and external regulatory environments. As governments and industry bodies introduce new cybersecurity regulations and standards, organizations face increasing pressure to demonstrate due diligence and accountability (Center for Internet Security, 2021). Yet regulatory compliance alone does not guarantee effective risk management, particularly in rapidly evolving threat landscapes. This tension between compliance and resilience has become a central theme in contemporary cybersecurity governance discourse (Swinton & Hedges, 2019).

Within this context, recent scholarship has called for more integrative and strategic approaches to cybersecurity governance that explicitly link risk assessment, policy formulation, and organizational decision-making. Mohammed Nayeem (2025) contributes to this discourse by proposing a strategic, risk-based policy framework that positions cybersecurity governance as a dynamic and iterative process. This framework emphasizes the alignment of cybersecurity

policies with organizational risk profiles, regulatory obligations, and strategic goals, offering a conceptual bridge between abstract governance principles and practical implementation.

Despite the growing body of work on cybersecurity governance, several gaps remain in the literature. First, there is a tendency to examine governance frameworks in isolation rather than exploring their complementarities and tensions. Second, many studies emphasize technical or behavioral dimensions without fully integrating strategic policy considerations. Third, there is limited synthesis of how risk-based governance can be operationalized across different organizational levels, from boards to operational teams. Addressing these gaps requires a comprehensive, theoretically grounded analysis that situates cybersecurity governance within broader enterprise governance and risk management paradigms.

This article responds to these challenges by developing an extensive, integrative examination of strategic risk-based cybersecurity governance. Drawing exclusively on the provided references, it seeks to articulate how policy frameworks, governance structures, and compliance mechanisms can be aligned to support effective cybersecurity risk management. By emphasizing theoretical elaboration, historical context, and critical debate, the study contributes to a deeper understanding of cybersecurity governance as a strategic organizational capability rather than a peripheral technical function (Mohammed Nayeem, 2025).

The remainder of the article is structured to support this objective. The methodology section outlines the qualitative, literature-driven approach used to synthesize and interpret governance frameworks and scholarly arguments. The results section presents a descriptive and interpretive analysis of key governance themes and patterns emerging from the literature. The discussion section offers an extensive theoretical integration, examining implications, limitations, and future research directions. The article concludes by summarizing key insights and reinforcing the strategic importance of risk-based cybersecurity governance in contemporary organizations.

METHODOLOGY

The methodological approach adopted in this study is qualitative, interpretive, and theory-driven, reflecting the conceptual and analytical nature of the research objective. Rather than seeking to test hypotheses through empirical measurement, the study aims to generate deep theoretical insight into strategic risk-based cybersecurity governance by synthesizing and critically analyzing existing scholarly and practitioner-oriented literature (Adam, Jusoh, & Streimikiene, 2019). This approach is particularly appropriate given the complexity of cybersecurity governance as a socio-technical phenomenon that encompasses organizational structures, policy frameworks, human behavior, and regulatory environments (Federal Virtual Training Environment, 2020).

At the core of the methodology is a structured literature analysis grounded exclusively in the references provided. These sources span academic journals, governance frameworks, policy guides, and practitioner analyses, offering a multifaceted perspective on cybersecurity governance. By deliberately restricting the data corpus to the specified references, the study ensures conceptual coherence and avoids introducing external theoretical assumptions that could dilute the analytical focus. This constraint also reinforces methodological rigor by requiring comprehensive engagement with each source rather than selective citation (Abbas et al., 2022).

The analytical process involved multiple iterative stages. First, each reference was examined to identify its primary theoretical orientation, governance assumptions, and conceptual contributions. Framework-oriented sources such as COBIT, NIST, ISO/IEC 27001, and CIS Controls were analyzed in terms of their governance logic, risk conceptualization, and policy implications (Calder, 2018; De Haes et al., 2019; Center for Internet Security, 2021; Edward, 2016). Scholarly articles were examined for empirical findings, theoretical arguments, and identified governance challenges, particularly those related to compliance behavior and board-level oversight (Cram et al., 2019; Al-sartawi, 2020).

Second, a thematic synthesis was conducted to identify recurring patterns and tensions across the literature. Themes such as risk-based decision-making, strategic alignment, policy integration, compliance limitations, and governance maturity emerged as central analytical categories (Swinton & Hedges, 2019; DataGuard, 2018). These themes served as analytical lenses through which individual sources were interpreted and compared. Importantly, the synthesis did not aim to homogenize perspectives but rather to highlight areas of convergence and divergence, thereby enriching theoretical debate (Adam et al., 2019).

Third, particular attention was given to integrative frameworks that explicitly connect cybersecurity governance with enterprise risk management and strategic policy formulation. Mohammed Nayeem (2025) was central to this stage of analysis, as the proposed risk-based policy framework provided a conceptual anchor for integrating disparate governance perspectives. The framework was not treated as a prescriptive model but as an analytical construct through which existing governance approaches could be evaluated and contextualized.

The methodology also incorporated a critical interpretive

stance. Rather than accepting governance frameworks and policy prescriptions at face value, the analysis interrogated their underlying assumptions, practical limitations, and contextual dependencies. For example, while compliance-oriented frameworks emphasize standardization and control, the literature reveals persistent challenges related to human behavior, organizational culture, and dynamic threat environments (Cram et al., 2019). A critical lens enables the exploration of these tensions and supports more nuanced theoretical conclusions.

Methodological limitations are acknowledged as an integral component of rigor. The exclusive reliance on secondary sources limits the ability to capture real-time organizational practices or emerging threats not reflected in the literature. Additionally, the absence of empirical data means that findings are interpretive rather than generalizable in a statistical sense. However, these limitations are consistent with the study's theoretical objectives and are mitigated by the depth and breadth of analytical engagement with authoritative sources (Abbas et al., 2021).

Overall, the methodology is designed to support an extensive, theoretically rich exploration of strategic cybersecurity governance. By combining structured literature analysis, thematic synthesis, and critical interpretation, the study provides a robust foundation for the descriptive and analytical results that follow (Mohammed Nayeem, 2025).

RESULTS

The results of this study emerge from an interpretive synthesis of the provided literature and reflect recurring governance patterns, conceptual alignments, and persistent challenges identified across scholarly and practitioner sources. Rather than presenting empirical measurements, the results articulate descriptive and analytical insights into how strategic risk-based cybersecurity governance is conceptualized and operationalized within contemporary organizations (Federal Virtual Training Environment, 2020).

A central finding is the widespread recognition that cybersecurity governance has evolved into a strategic concern that transcends technical implementation. Multiple sources emphasize that effective governance requires active involvement from senior leadership and boards, reflecting a shift toward enterprise-wide accountability for cybersecurity risk (Al-sartawi, 2020; Swinton & Hedges, 2019). This shift is driven by the increasing materiality of cyber risks, which can result in financial losses, reputational damage, and regulatory sanctions. As a result, cybersecurity is no longer viewed solely as an IT function but as an integral component of organizational governance structures (De Haes et al., 2019).

Another significant result relates to the prominence of risk-based approaches within contemporary governance frameworks. The NIST Cybersecurity Framework, COBIT, and CIS Controls all emphasize risk assessment and prioritization as foundational governance principles (Calder, 2018; De Haes et al., 2019; Center for Internet Security, 2021). These frameworks encourage organizations to tailor security controls to their specific risk profiles rather than adopting uniform, prescriptive measures. The literature consistently highlights this flexibility as a key strength, enabling organizations to align cybersecurity investments with strategic objectives and risk tolerance (DataGuard, 2018).

However, the results also reveal persistent tensions between risk-based governance ideals and compliance-driven practices. Empirical analyses of policy compliance behavior indicate that employees often perceive security policies as burdensome or misaligned with operational realities, leading to inconsistent adherence (Cram et al., 2019). This finding underscores a critical governance challenge: policies designed without sufficient consideration of human behavior and organizational context may undermine their own effectiveness. Risk-based governance frameworks acknowledge this issue but often provide limited guidance on addressing behavioral and cultural factors in practice (Edward, 2016).

The analysis further indicates that board-level engagement in cybersecurity governance remains uneven. While there is growing awareness of cyber risk at the board level, many boards lack the expertise required to critically evaluate cybersecurity strategies and risk assessments (Al-sartawi, 2020). This knowledge gap can result in symbolic governance, where cybersecurity is discussed at a high level without substantive oversight or integration into enterprise risk management processes. The literature suggests that effective governance requires not only formal structures but also capacity-building and ongoing education for senior leaders (Swinton & Hedges, 2019).

A notable result concerns the role of strategic policy frameworks in bridging the gap between technical controls and organizational governance. Mohammed Nayeem (2025) emphasizes that risk-based policy frameworks serve as translation mechanisms, converting technical risk assessments into actionable governance decisions. This perspective resonates with broader governance literature, which highlights the importance of policies as instruments for aligning organizational behavior, accountability, and strategic intent (Federal Virtual Training Environment, 2020). The analysis suggests that organizations with coherent, risk-informed policy architectures are better positioned to adapt to evolving threats and regulatory expectations.

The results also highlight the increasing interconnection

between cybersecurity governance and external regulatory environments. Compliance with standards such as ISO/IEC 27001 and adherence to recognized frameworks are often used as proxies for due diligence and good governance (Edward, 2016). However, the literature cautions against equating compliance with security effectiveness, particularly in dynamic threat landscapes characterized by novel attack vectors such as ransomware (Alejandro et al., 2019). This finding reinforces the argument that risk-based governance must remain adaptive and forward-looking rather than static and retrospective.

Finally, the synthesis reveals a growing emphasis on integration and coordination across organizational functions. Effective cybersecurity governance is portrayed as a cross-functional endeavor involving IT, risk management, legal, compliance, and business units (De Haes et al., 2019). Fragmented governance structures, where responsibilities are siloed, are associated with gaps in risk visibility and delayed response to incidents. Risk-based governance frameworks seek to address this fragmentation by providing shared language and decision-making structures centered on risk (Mohammed Nayeem, 2025).

Collectively, these results illustrate that while conceptual consensus around strategic, risk-based cybersecurity governance is emerging, practical implementation remains uneven and contested. The findings provide a foundation for deeper theoretical interpretation and critical discussion in the following section.

DISCUSSION

The discussion of strategic risk-based cybersecurity governance necessitates a deep theoretical engagement with governance theory, risk management scholarship, and organizational behavior literature. The results presented earlier reveal both convergence and tension within contemporary cybersecurity governance discourse, underscoring the complexity of translating abstract frameworks into effective organizational practice (Swinton & Hedges, 2019). This section critically interprets these findings, situating them within broader scholarly debates and exploring their implications for theory, policy, and future research.

At a theoretical level, cybersecurity governance can be understood as an extension of enterprise governance of IT, a concept that emphasizes the alignment of information systems with organizational strategy, value creation, and risk optimization (De Haes et al., 2019). Traditional IT governance models focused primarily on efficiency, control, and standardization. However, the escalation of cyber threats has expanded the governance agenda to include resilience, adaptability, and strategic foresight. Risk-based cybersecurity governance reflects this evolution by positioning risk as the central organizing principle around which policies, controls, and decision-making processes are structured (Calder, 2018).

One of the most significant theoretical contributions of risk-based governance is its challenge to compliance-centric paradigms. Compliance-based approaches are rooted in institutional theory, which suggests that organizations adopt standardized practices to gain legitimacy and meet external expectations (Edward, 2016). While such practices can promote baseline security hygiene, they may also encourage a checkbox mentality that prioritizes formal adherence over substantive risk reduction. The literature reviewed consistently highlights this limitation, particularly in contexts where regulatory requirements lag behind emerging threats (DataGuard, 2018).

Risk-based governance, by contrast, aligns more closely with contingency theory, which posits that organizational effectiveness depends on contextual fit rather than universal prescriptions. Frameworks such as NIST and COBIT embody this logic by encouraging organizations to tailor controls based on risk assessments, business objectives, and threat environments (De Haes et al., 2019). Mohammed Nayeem (2025) advances this perspective by emphasizing strategic policy frameworks that explicitly integrate risk intelligence into governance processes. This approach not only enhances adaptability but also supports strategic decision-making by framing cybersecurity investments in terms of risk trade-offs and organizational priorities.

Despite its theoretical appeal, risk-based governance raises important practical and ethical questions. One concern relates to the subjectivity of risk assessment. Risk is inherently probabilistic and influenced by assumptions, perceptions, and available information. Boards and senior executives may struggle to interpret technical risk assessments, leading to either overestimation or underestimation of threats (Al-sartawi, 2020). This challenge underscores the importance of governance mechanisms that facilitate shared understanding and transparent communication between technical experts and decision-makers.

Another area of scholarly debate concerns the human dimension of cybersecurity governance. Behavioral research indicates that employee compliance with security policies is influenced by factors such as perceived fairness, usability, and organizational culture (Cram et al., 2019). Risk-based policies that fail to account for these factors may inadvertently increase vulnerability by encouraging workarounds or non-compliance. The literature suggests that effective governance must integrate formal controls with informal mechanisms such as training, leadership example, and cultural reinforcement (Federal Virtual Training Environment, 2020).

The discussion also highlights the strategic role of boards in cybersecurity governance. Board-level oversight is widely regarded as a cornerstone of effective governance, yet empirical evidence suggests that many boards lack the expertise or confidence to engage deeply with cybersecurity issues (Al-sartawi, 2020). This gap has prompted calls for enhanced board education, the inclusion of cybersecurity expertise in board composition, and the development of governance dashboards that translate technical metrics into strategic insights (Swinton & Hedges, 2019). Risk-based frameworks support these initiatives by providing a common language for discussing cybersecurity in terms of enterprise risk.

From a policy perspective, the integration of cybersecurity governance with regulatory compliance remains a contested issue. Regulatory frameworks often emphasize minimum standards and reporting requirements, which may not align with organizational risk profiles or strategic objectives (Edward, 2016). The literature reviewed suggests that organizations should view compliance as a baseline rather than an endpoint, using risk-based governance to extend beyond regulatory minima toward proactive risk management (Center for Internet Security, 2021). Mohammed Nayeem (2025) reinforces this view by positioning policy frameworks as dynamic instruments that evolve in response to both regulatory changes and threat intelligence.

The discussion further reveals tensions between centralization and decentralization in cybersecurity governance. Centralized governance structures can promote consistency, visibility, and accountability, while decentralized approaches may enhance responsiveness and contextual awareness (De Haes et al., 2019). Risk-based governance offers a potential reconciliation by establishing centralized risk principles and policies while allowing localized implementation tailored to specific operational contexts. This balance is particularly important in large, complex organizations with diverse information systems and risk exposures.

Limitations of the current theoretical landscape are also evident. Much of the existing literature focuses on frameworks and best practices without sufficiently addressing the political and power dynamics that shape governance outcomes. Decision-making authority, resource allocation, and accountability structures can influence how risk-based policies are interpreted and enforced. Future research could benefit from incorporating perspectives from organizational politics and critical management studies to deepen understanding of these dynamics (Adam et al., 2019).

In terms of future research directions, the findings suggest several promising avenues. Longitudinal studies could examine how organizations transition from compliance-based to risk-based governance models over time, capturing learning processes and adaptation. Comparative studies across sectors and regulatory regimes could illuminate contextual factors that influence governance effectiveness. Additionally, interdisciplinary research integrating insights from psychology, sociology, and public policy could enrich understanding of the human and institutional dimensions of cybersecurity governance (Abbas et al., 2022).

Overall, the discussion underscores that strategic risk-based cybersecurity governance is not a static destination but an ongoing process of alignment, learning, and adaptation. While frameworks and policies provide essential scaffolding, their effectiveness ultimately depends on organizational commitment, leadership engagement, and the capacity to integrate risk intelligence into strategic decision-making (Mohammed Nayeem, 2025).

CONCLUSION

This research article has developed an extensive theoretical and analytical examination of strategic risk-based cybersecurity governance, grounded strictly in the provided scholarly and practitioner-oriented references. The analysis demonstrates that cybersecurity governance has evolved into a central component of enterprise governance, requiring active board-level oversight, strategic policy integration, and continuous risk assessment. Risk-based governance frameworks offer a compelling alternative to compliance-centric approaches by aligning cybersecurity activities with organizational objectives and threat environments (Calder, 2018; De Haes et al., 2019).

The findings highlight both the promise and the challenges of risk-based governance. While frameworks such as NIST, COBIT, ISO/IEC 27001, and CIS Controls provide valuable guidance, their effectiveness depends on contextualization, human behavior, and organizational culture. Strategic policy frameworks, as articulated by Mohammed Nayeem (2025), play a critical role in translating technical risk insights into governance decisions that support resilience and accountability.

By synthesizing diverse governance perspectives and engaging critically with scholarly debates, this article contributes to a deeper understanding of cybersecurity governance as a dynamic, strategic capability. It underscores the need for organizations to move beyond static compliance toward adaptive, risk-informed governance models capable of responding to evolving cyber threats. Future research and practice should continue to explore how governance structures, policies, and leadership practices can be aligned to foster sustainable cybersecurity resilience in an increasingly interconnected digital world.

REFERENCES

1. Alejandro, C., Guarda, T., & Ninahualpa Quiña, G. (2019). Ransomware – WannaCry security is everyone's.

2. De Haes, S., Van Grembergen, W., Joshi, A., & Huygh, T. (2019). COBIT as a framework for enterprise governance of IT.

3. Abbas, A. F., Jusoh, A., Mas, A., Alsharif, A. H., & Ali, J. (2022). Bibliometrix analysis of information sharing in social media. Cogent Business & Management, 9(1).

4. Mohammed Nayeem. (2025). Strategic Cybersecurity Governance: A Risk-Based Policy Framework for IT Protection and Compliance. In Proceedings of the International Conference on Artificial Intelligence and Cybersecurity (ICAIC 2025), 19–29.

5. Edward, H. (2016). Implementing the ISO/IEC 27001:2013 ISMS Standard.

6. Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. MIS Quarterly, 43(2), 525–554.

7. DataGuard. (2018). Cyber security governance: Policies, processes and controls for businesses.

8. Center for Internet Security. (2021). CIS Controls v8.

9. Al-sartawi, A. M. A. M. (2020). Information technology governance and cybersecurity at the board level. International Journal of Critical Infrastructures, 16(2), 150–161.

10. Swinton, S., & Hedges, S. (2019). Cybersecurity governance, Part 1: 5 fundamental challenges. SEI Blog.

11. Federal Virtual Training Environment. (2020). Cybersecurity governance.

12. Abbas, A. F., Jusoh, A., Masod, A., Ali, J., Ahmed, H., & E, A. R. H. (2021). A bibliometric analysis of publications on social media influencers. Journal of Theoretical and Applied Information Technology, 99(23), 5662–5676.

13. Adam, I., Jusoh, A., & Streimikiene, D. (2019). Scoping research on sustainability performance from manufacturing industry sector. Problems and Perspectives in Management, 17(2).