INTERNATIONAL JOURNAL OF DIGITAL BUSINESS AND STRATEGY

NAWALA

Volume 2, Number 1, 2023

IT Security Governance for Digital Enterprises: Balancing Agility and Control

Cindi Mutia [1]

[1] Universitas Sarjanawiyata Tamansiswa, Yogyakarta, Indonesia

Abstract

Article history:
Received: January 14, 2023
Revised: February 5, 2023
Accepted: April 17, 2023
Published: June 30, 2023

Keywords:
Agility
Control
Cybersecurity Strategy
Digital Enterprise
IT Security Governance

Identifier:
Nawala
Page: 1-14
https://nawala.io/index.php/ijdbs

Digital transformation has revolutionized the way organizations manage information, but it also presents complex challenges when it comes to security. This study explores how IT Security Governance can balance the need for agility and control in the context of digital enterprises. The method used is a literature study of twenty selected scientific publications published in the last five years. Studies show that traditional rigid approaches to security management are no longer adequate in dealing with today's technological dynamics. Adaptive approaches such as Zero Trust Architecture, DevSecOps, and policy-as-code are emerging as key strategies for maintaining flexibility without sacrificing compliance and control. In addition, the culture of security and the involvement of all stakeholders play a crucial role in the success of governance. The results of this study provide a conceptual and practical understanding of how organizations can build security systems that are resilient, responsive, and relevant to the ever-changing digital age.

*Corresponding author:
(Cindi Mutia)

1. Introduction

The rapid development of information technology in the digital era has presented new challenges and opportunities for modern organizations, especially in terms of IT Security Governance. In the midst of rapid digital transformation, organizations are faced with the need to remain adaptive and agile in responding to market and technological changes. However, at the same time, they are required to maintain strict control over information security systems to prevent the risk of data leaks, cyberattacks, and regulatory compliance failures. The tension between the need for agility and control has become a strategic dilemma in managing information security in digital enterprises today. According to Kartheeyayini et al. (2022), many digital organizations are now looking to modernize their IT infrastructure through a cloud-native approach and Zero Trust Architecture (ZTA) to support scalability and flexibility without sacrificing control and compliance aspects.

Concepts like Azure Landing Zones not only provide scalable cloud-based infrastructure governance, but also include built-in security mechanisms to address governance challenges in the digital context. This shows that the success of digital transformation is closely related to how organizations balance two seemingly opposite poles: agility and control. Research by Anene and Clement (2022) confirms that in the context of enterprise hybrid cloud, enterprises need a governance approach that is not only compliance-oriented, but also supports the operationalization of DevOps strategies, AI/ML-based security, and policy automation. Traditional governance models that are rigid and hierarchical are no longer adequate in dealing with the complexity of today's technology. On the

contrary, an adaptive and modular approach allows for a balance to be created between the need for rapid innovation and the protection of information assets.

In the SME (Small and Medium Enterprises) sector, a study by Carayannis et al. (2019) shows that cost-effective and agile security governance is a must due to limited resources. The use of dynamic risk mitigation strategies such as managed security services, culture-based security training, and risk monitoring automation are best practices that emerge from these limitations. This concept is also in line with the idea that agility does not necessarily ignore control, but integrates it intelligently and contextually. On the other hand, the pressures from regulations such as GDPR, ISO 27001, NIST CSF, and various international standards encourage companies to maintain a high level of control in every digital initiative. As explained by Jayasinghe et al. (2022), the main challenge in digital transformation is not only the adoption of new technologies, but also in how organizations build digital resilience and the ability to survive and thrive in the midst of increasing cyber threats.

Digital resilience is formed through a synergy between agility that accelerates organizational response and control that maintains stability and user trust. Digital companies also face increasingly complex external pressures, ranging from automated ransomware attacks to third-party system integrations that increase the attack surface. Therefore, the approach to security governance can no longer be one-way or reactive. A governance model is needed that is holistic, iterative, and able to adapt to the ever-changing risk landscape. Kanbar and Faraj (2022) argue that in multi-cloud and hybrid environments, the ability to manage load balancing securely and efficiently becomes an integral part of security and control strategies.

The main objective of this literature review is to review and synthesize various approaches, frameworks, and best practices in information security governance for digital enterprises, with a particular focus on how organizations balance the need for agility and control. This study will analyze the current academic literature (2019–2022) to identify trends, challenges, technical and policy solutions, and their impact on organizations capabilities in achieving sustainable security in the digital age. By combining perspectives from academic research and industry practice, this study is expected to make a conceptual and practical contribution to the development of IT Security Governance strategies that are responsive, contextual, and adaptive to digital dynamics. This approach is not only important for large organizations, but it is also particularly relevant for medium and small companies that want to stay competitive amid global digital transformation.

2. Methods

This study uses the literature review method as the main approach to study and analyze the topic "IT Security Governance for Digital Enterprises: Balancing Agility and Control". The literature study method was chosen because it allows researchers to examine various published scientific sources to understand trends, problems, approaches, and solutions that have been developed in a certain period of time. The focus of the study is directed at the literature based on Google Scholar, Research Gate and Elsevier, published in last five years to ensure relevance to the contemporary digital context, especially in the post-COVID-19 pandemic digital transformation period that accelerates the adoption of cloud, edge computing, and

hybrid work models. The main sources used in this study include scientific journal articles, conference proceedings.

Inclusion criteria are set to ensure the quality and relevance of sources, including: the article is written in English or Indonesian; published in last five years ; the focus of the discussion on the topics of IT security governance, digital transformation, cybersecurity control, and technology-based risk management models; and have citations or have been used as references in similar research. The search technique was carried out using keywords such as "IT security governance", "digital enterprises", "cybersecurity agility", "risk control", "adaptive governance frameworks", and "hybrid cloud security". After the initial search process, an initial selection process is carried out through abstract reading to identify the relevance of the content to the topic. Eligible articles are then read thoroughly for content analysis and extraction of critical information that includes approaches, frameworks, challenges, and policy recommendations.

The data synthesis process is carried out using a thematic approach, where the content of the literature is categorized into main themes such as governance models, balance between agility and control, implementation in cloud-native architectures, to risk management and regulatory compliance. In addition, research gaps are also identified and approaches are compared to assess their strengths and weaknesses in the context of digital organizations. In an effort to improve the validity and credibility of the analysis, only literature that comes from reputable sources and has gone through a peer-review process is included. The data obtained was not analyzed quantitatively, but through a qualitative-descriptive approach with

an interpretation of the content and arguments built by each author. The results of this literature synthesis will be presented in Chapter III, which is divided into three main subchapters: Basic Concepts and Evolution of IT Security Governance, Practical Challenges in Balancing Agility and Control, and Implementation Strategies in Modern Digital Organizations.

3. Results

3.1. The Concept and Evolution of IT Security Governance

IT Security Governance (ITSG) is a part of information technology governance that focuses on the security, integrity, and confidentiality of an organization's information. In the context of digital enterprises, ITSG's role has evolved from a mere technical oversight function to a strategic element that directly supports digital transformation and business sustainability. This evolution is triggered by changes in the technology ecosystem, such as the increased use of cloud computing, IoT, artificial intelligence, and the adoption of hybrid work models post-pandemic. According to Soomro et al. (2021), traditional governance approaches that are hierarchical and centralized are no longer effective in dealing with fast and dynamic business needs.

Therefore, digital organizations are starting to adopt an adaptive and risk-based governance model. Modern governance emphasizes flexibility, cross-functional integration, and ongoing collaboration between security, development, and business teams. Frameworks such as COBIT 2019, the NIST Cybersecurity Framework, and ISO/IEC 27001 are still the main references, but their

implementation is now being adjusted to be more dynamic. Artyushina (2020) reveal that digital organizations need a governance framework that allows for periodic evaluation and adjustment of security controls, in accordance with changes in technology and regulations.

Sarker et al. (2022) also stated that to achieve security resilience, organizations need to build hybrid security models, especially in IoT-based systems and edge computing. Cloud-native architectures also encourage policy-as-code-based governance (Odun-Ayo et al., 2019), which allows security policies to be designed as code that can be tested, audited, and executed automatically. It is also important to understand that ITSG does not only include technical tools, but also covers aspects of organizational governance as a whole including leadership structures, roles and responsibilities, and security culture. Brass and Sowell (2021) explained that effective governance requires active involvement from all lines of the organization, from executives to end users.

In a long-term perspective, ITSG must also be sustainable and business-value-oriented. Good governance is not only aimed at reducing risks, but also creating digital trust which is the main capital in the digital economy ecosystem. According to De Haes et al. (2020), governance that is responsive to risks while supporting innovation will provide a competitive advantage for digital organizations. Thus, ITSG in digital companies is no longer just a control procedure, but a strategic management system that continues to evolve following the direction of technological transformation and global business needs. This evolution shows that

security and innovation do not have to be in conflict with each other, but can reinforce each other within the right governance framework.

3.2. Practical Challenges in Balancing Agility and Control

Digital companies face a complex dilemma in maintaining a balance between agility and control. On the one hand, organizations need to innovate quickly to stay competitive. On the other hand, they must maintain data security and compliance with increasingly stringent regulations. The tension between these two needs often triggers strategic and operational conflicts within the organization. One of the most prominent challenges is the integration of security into agile business processes. In a DevOps environment, application development and deployment are done quickly and iteratively. If security controls are not integrated from the start, then the risk of data leakage or misuse increases. DevSecOps approach is present as a solution, but it requires a major change in the organizational structure and team mindset.

On the other hand, an overly restrictive security approach can hinder business agility. Davis (2021) emphasizes that too much bureaucracy and manual control can slow innovation, lower team motivation, and increase the risk of shadow IT, where employees use technology without the knowledge of the IT department. Battina (2021) shows that the communication gap between the security team and the development team is also a serious obstacle. Non-inclusive governance often ignores the operational context, making the policies implemented irrelevant or difficult to implement.

Another aspect that is no less important is the limitation of resources, especially in small and medium enterprises (SMEs). Carayannis et al. (2019)

mentioned that many SMEs do not have enough personnel or budget to implement complex security frameworks. This causes SMEs to have to choose between speed or protection, even though both are equally vital. From a technology perspective, the use of multi-cloud and hybrid clouds creates new challenges in managing access controls, log audits, and network segmentation. Kanbar and Faraj (2022) state that the lack of interoperability between cloud platforms complicates the implementation of governance, particularly in terms of consistency of security policies across systems.

Organizational culture also plays an important role. Arbanas et al. (2021) explained that without a strong embedded security culture, governance efforts will tend to be formal. Users who are not aware of the risks are often a major weak point in the security system. Regulations that continue to change are also a challenge in itself. Standards like GDPR, HIPAA, and ISO27001 provide a compliance framework, but their interpretation is not always clear. This can lead to uncertainty in decision-making, as explained by Jayasinghe et al. (2022) in their study of the banking sector. Faced with these challenges, digital companies need to realize that balancing agility and control is not a short-term project, but rather an ongoing process that requires strong cross-functional evaluation, adaptation, and collaboration.

3.3. Governance Implementation Strategy in Digital Organizations

In facing the challenge of balancing agility and control, digital organizations need to implement an adaptive, scalable, and risk-based IT Security Governance strategy. The strategy must integrate technical, process, and cultural approaches to

create a security system that not only protects but also encourages innovation. One key approach is the adoption of DevSecOps, where security is built into the entire software development lifecycle. Kartheeyayini et al. (2022) state that the use of Azure Landing Zones and CI/CD pipelines equipped with automated security controls allows for the effective application of shift-left security principles. The policy-as-code approach is also becoming more popular.

By writing policies as code, organizations can integrate security controls in the automation process, avoid manual errors, and increase the speed of audits (Anene & Clement, 2022). This is especially important in multi-cloud scenarios and complex microservices architectures. Risk-based governance strategies are increasingly being adopted by companies of different scales and capacities. Carayannis et al. (2019) emphasizes that this approach allows SMEs to set controls according to the level of risk, not just based on universal standards. Thus, resources can be used more efficiently and on target. The application of supporting technologies such as SIEM (Security Information and Event Management), CASB (Cloud Access Security Broker), EDR (Endpoint Detection and Response), and AI-based threat analytics play a critical role in creating an adaptive and data-driven security response.

Loft et al. (2022) added that real-time security dashboards help management make quick and informed decisions. Adaptive governance engine framework that is capable of reconfiguring security controls based on changing risks and business contexts. This approach is particularly useful in organizations that operate globally and face cross-border regulations. In addition to the technical aspects, organizations need to strengthen the security culture with ongoing training. Arbanas et al. (2021)

suggest the use of phishing simulations and gamification approaches to increase user awareness. A strong security culture accelerates the adoption of new policies and lowers the risk of insider threats.

Finally, standard frameworks such as NIST CSF, COBIT 2019, and ISO/IEC 27001 remain relevant, but their implementation must be flexible and contextual. Pinto-Albuquerque & Fonseca (2021) emphasize that a framework will only be effective if it is aligned with the business processes and strategic needs of the organization. By combining technical, human, and process aspects in an integrated governance strategy, digital organizations can build security systems that are resilient, agile, and ready to face the risk dynamics in the digital age.

4. Conclusion

In the era of digital transformation that continues to grow, organizations are not only required to move quickly and adaptively, but must also be able to protect information assets effectively and sustainably. This literature review examines the approach and practice of IT Security Governance (ITSG) that is able to balance two crucial needs: agility and control in digital organizations. The results of the study show that traditional governance models that are centralistic and static are no longer effective in dealing with the complexity of current technologies such as cloud-native architecture, DevOps, and multi-cloud environments.

Instead, models that are adaptive, risk-based, and automated are becoming more relevant and efficient. Integration of approaches such as Zero Trust Architecture, DevSecOps, policy-as-code, and multi-level governance has been

proven to help organizations maintain the speed of innovation without sacrificing security and compliance controls. However, the implementation of this strategy is not without challenges. Key barriers include limited resources, lack of security literacy, organizational cultural resistance, and gaps between regulation and operational implementation.

In terms of human resources, continuous training and strengthening the organization's security culture are key in creating resilient governance. Supporting technologies such as security automation, SIEM, EDR, and AI-based threat detection are increasingly important in creating adaptive and data-driven security controls. On the other hand, international frameworks such as NIST CSF, ISO 27001, and COBIT 2019 remain important references, but they need to be contextually adapted. Overall, the ideal IT Security Governance is governance that not only encourages compliance and protection, but also supports continuous innovation. Organizations that are able to balance agility and control will be better prepared to face security challenges in a dynamic and high-risk digital age.

References

Anene, U. N., & Clement, T. (2022). A resilient logistics framework for humanitarian supply chains: Integrating predictive analytics, IoT, and localized distribution to strengthen emergency response systems. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *8*(5), 398-424.

Arbanas, K., Spremic, M., & Zajdela Hrustek, N. (2021). Holistic framework for evaluating and improving information security culture. *Aslib Journal of Information Management*, *73*(5), 699-719.

Artyushina, A. (2020). Is civic data governance the key to democratic smart cities? The role of the urban data trust in Sidewalk Toronto. *Telematics and Informatics*, *55*, 101456.

Battina, D. S. (2021). The challenges and mitigation strategies of using DevOps during software development. *International Journal of Creative Research Thoughts (IJCRT), ISSN*, 2320-2882.

Brass, I., & Sowell, J. H. (2021). Adaptive governance for the Internet of Things: Coping with emerging security risks. *Regulation & Governance*, *15*(4), 1092-1110.

Carayannis, E. G., Grigoroudis, E., Rehman, S. S., & Samarakoon, N. (2019). Ambidextrous cybersecurity: The seven pillars (7Ps) of cyber resilience. *IEEE transactions on engineering management*, *68*(1), 223-234.

Davis, R. E. (2021). *Auditing Information and Cyber Security Governance: A Controls-based Approach*. Florida : CRC Press.

De Haes, S., Caluwe, L., Huygh, T., & Joshi, A. (2020). *Governing Digital Transformation, Guidance for Corporate Board Members.* Springer.

Jayasinghe, N., Fernando, S., Haigh, R., Amaratunga, D., Fernando, N., Vithanage, C., ... & Ranawana, C. (2022). Economic resilience in an era of 'systemic risk': Insights from four key economic sectors in Sri Lanka. *Progress in Disaster Science*, *14*, 100231.

Kanbar, A. B., & Faraj, K. (2022). Region aware dynamic task scheduling and resource virtualization for load balancing in IoT–fog multi-cloud environment. *Future Generation Computer Systems*, *137*, 70-86.

Kartheeyayini, V., Madhumitha, S., Lalitha, G., Jackulin, C., & Subramanian, K. (2022, May). AWS cloud computing platforms deployment of landing zone-Infrastructure as a code. In *AIP Conference Proceedings* (Vol. 2393, No. 1, p. 020175). AIP Publishing LLC.

Loft, P., He, Y., Yevseyeva, I., & Wagner, I. (2022). CAESAR8: An agile enterprise architecture approach to managing information security risks. *Computers & Security*, *122*, 102877.

Odun-Ayo, I., Goddy-Worlu, R., Ajayi, L., Edosomwan, B., & Okezie, F. (2019, December). A systematic mapping study of cloud-native application design and engineering. In *Journal of Physics: Conference Series* (Vol. 1378, No. 3, p. 032092). IOP Publishing.

Sarker, P. S., Sadanandan, S. K., & Srivastava, A. K. (2022). Resiliency metrics for monitoring and analysis of cyber-power distribution system with IoTs. *IEEE Internet of Things Journal*, *10*(9), 7469-7479.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2021). Information security governance: A systematic literature review and future research directions. *Computers & Security*, 103,