GASET
GLOBAL ADVANCES IN SCIENCE, ENGINEERING & TECHNOLOGY

E-ISSN: 3123-724x
Volume 2, **Number** 1, June 2026
https://doi.org/10.62671/ gaset.v2i1.289

Analysis of Information Security, Privacy, and Legality of Use in Modern Digital Transformation

Nadya Lathifah Riady[1], Evy Nurmiati[2]
[1,2] Universitas Islam Negeri Syarif Hidayatullah Jakarta, Indonesia
[1]nadyariady71@gmail.com, [2]evy.nurmiati@uinjkt.ac.id

open access

***Corresponding Author**

Article History:
Submitted: 10 June 2026
Accepted: 23 June 2026
Published: 25 June 2026

Keywords:
cyber security, data protection, information security, legal compliance, privacy.

ABSTRACT

The rapid growth and pervasive integration of digital technology in global sectors have significantly increased the vulnerability of organizational data, placing a paramount importance on information security, privacy preservation, and strict legal compliance. This study aims to examine the systemic relationship between these three critical dimensions within modern digital ecosystems, identifying core vulnerabilities and assessing regulatory efficacy. The research employs a qualitative methodology through a systematic literature review of highly credible scientific publications indexed between 2022 and 2024. The empirical findings indicate that weak database encryption architecture, low user cybersecurity awareness, and inconsistent legal enforcement frameworks are the primary socio-technical factors contributing to massive data breaches and proliferating cybercrimes. Furthermore, strict alignment with contemporary data protection regulations plays an indispensable role in safeguarding user privacy and compelling organizations to adopt proactive security posturing. However, a significant enforcement gap remains between comprehensive legal provisions and practical execution capabilities, particularly within public institutions and small-scale business sectors. This study highlights the urgent need for integrated, triple-helix collaborative strategies that combine technological innovations, comprehensive institutional policy frameworks, and continuous user awareness education to build a secure, resilient, and trusted digital ecosystem.

INTRODUCTION

Digital transformation is a global phenomenon that has fundamentally reshaped the way individuals interact, work, and manage information. The rapid advancement of information and communication technologies, including the Internet, cloud computing, big data, the Internet of Things (IoT), and artificial intelligence (AI), has accelerated the integration of digital systems across various sectors, including business, education, healthcare, government, and industry. The adoption of digital technologies has enabled organizations to improve operational efficiency, enhance decision-making processes, and expand access to public services and information in real time. Furthermore, digitalization has fostered the emergence of innovative business models that are more adaptive and competitive in the global marketplace (Susanto et al., 2022; Zhang & Chen, 2023).

Despite its numerous benefits, digital transformation also presents increasingly complex challenges, particularly in relation to information security, privacy protection, and legal compliance. In the digital economy, data has become a strategic asset with substantial economic value. Modern organizations rely heavily on data to support business operations, service development, and decision-making processes. Consequently, security breaches and cyber incidents can directly affect organizational sustainability, corporate reputation, and public trust in digital services (Alharbi et al., 2022).

The widespread adoption of digital technologies has been accompanied by a significant increase in both the frequency and sophistication of cyber threats. Various forms of cyberattacks, including phishing, malware, ransomware, distributed denial-of-service (DDoS) attacks, identity theft, and data breaches, continue to evolve with increasingly advanced techniques. Recent reports indicate a substantial rise in cybersecurity incidents targeting personal data and critical digital infrastructures. Sensitive information such as national identification numbers, financial records, online behavioral data, and healthcare information has become a primary target due to its high value in illicit digital markets and dark web ecosystems (Kumar & Singh, 2023; ENISA, 2024).

Beyond information security concerns, digital privacy has emerged as a critical issue in contemporary digital transformation. The collection, storage, and processing of vast amounts of personal data often raise concerns regarding

E-ISSN: 3123-724x
Volume 2, **Number** 1, June 2026
https://doi.org/10.62671/ gaset.v2i1.289

unauthorized access and misuse. Many digital platforms gather user information for behavioral analytics, service personalization, and targeted marketing purposes. However, the lack of transparency regarding how personal information is collected, processed, and shared may lead to significant privacy risks. Therefore, protecting personal data has become a crucial factor in fostering user trust and ensuring the sustainable development of digital ecosystems (Nguyen et al., 2022).

From a legal perspective, many countries have established regulatory frameworks to govern the protection and management of personal data. In Indonesia, personal data protection is regulated under Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), which provides a legal foundation for the collection, processing, storage, and dissemination of personal information. The regulation aims to strengthen data security practices and provide legal certainty for both individuals and electronic system operators. At the international level, the General Data Protection Regulation (GDPR) serves as a benchmark for implementing stringent data protection standards. Compliance with these regulations poses significant challenges for organizations, requiring investments in cybersecurity technologies, policy development, governance frameworks, and human resource competencies.

In addition to technological and regulatory factors, the human factor plays a pivotal role in determining the overall security posture of information systems. Numerous studies have shown that a considerable proportion of cybersecurity incidents result from human errors, such as weak password practices, susceptibility to phishing attacks, and inadequate awareness of cybersecurity best practices. Low levels of digital literacy often make users the weakest link in the information security chain. Consequently, enhancing cybersecurity awareness and digital literacy has become essential for establishing a sustainable culture of security within organizations and society (Nguyen et al., 2022).

Considering these challenges, a comprehensive examination of information security, digital privacy, and legal compliance within the context of modern digital transformation is essential. Such an investigation is necessary to identify emerging threats, evaluate the effectiveness of existing regulatory frameworks, and formulate strategic recommendations for developing a secure, trustworthy, and sustainable digital ecosystem. Ultimately, digital transformation should not only promote innovation and operational efficiency but also ensure the protection of personal data and the preservation of users' rights in an increasingly interconnected and complex digital environment.

Furthermore, privacy concerns have become increasingly critical as technological advancements enhance the capability to collect, store, process, and analyze vast amounts of data. Technologies such as big data analytics and artificial intelligence enable organizations to derive valuable insights from user-generated data, thereby improving decision-making processes and service personalization. However, without appropriate governance and safeguards, these capabilities may pose significant risks to individual privacy. Numerous cases have demonstrated that personal data are often collected, processed, or shared without explicit user consent and, in some instances, misused for commercial, political, or other unauthorized purposes (Rahman et al., 2023).

The legal dimension also plays a crucial role in regulating the use of digital technologies and ensuring the protection of personal data. In response to emerging challenges associated with digital transformation, many countries have established comprehensive regulatory frameworks. Examples include the General Data Protection Regulation (GDPR) in the European Union and Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) in Indonesia. These regulations are intended to provide legal safeguards for personal information and ensure that data processing activities are conducted in a transparent, accountable, and responsible manner (Putri & Santoso, 2023). Nevertheless, the implementation of such regulations continues to face several challenges, including limited awareness among industry stakeholders, insufficient organizational resources, and weaknesses in monitoring, compliance, and law enforcement mechanisms (Wibowo et al., 2024).

Issues related to information security, privacy, and legal compliance in the context of digital transformation are inherently multidimensional and highly interconnected. Weak security measures may result in privacy breaches, while inadequate regulations or ineffective law enforcement can further exacerbate these vulnerabilities. Conversely, even robust regulatory frameworks may prove ineffective if they are not supported by appropriate technological safeguards and a high level of user awareness (Sari et al., 2022). Moreover, the rapid pace of digital transformation necessitates a careful balance between technological innovation and the protection of users' rights. Many organizations prioritize the enhancement of digital services and operational efficiency while paying insufficient attention to comprehensive security and privacy considerations. Consequently, new and previously unidentified risks continue to emerge. Therefore, a holistic

E-ISSN: 3123-724x
Volume 2, **Number** 1, June 2026
https://doi.org/10.62671/ gaset.v2i1.289

approach is essential to ensure that digital transformation not only delivers technological and economic benefits but also maintains user trust, security, and privacy.

Although numerous studies have examined information security, privacy, and legal compliance individually, research that integrates these three dimensions within a comprehensive analytical framework remains relatively limited. This gap highlights the need for further investigation into the complex relationships among these factors in the context of digital transformation. Accordingly, this study addresses several key research questions, including the relationship between information security, privacy, and legal compliance in digital transformation; the factors influencing security incidents and privacy violations; and the role of regulatory frameworks in supporting personal data protection in the digital era.

In line with these research problems, this study aims to analyze the interrelationship between information security, privacy, and legal compliance within the digital transformation landscape. It further seeks to identify factors contributing to security risks and privacy violations and to evaluate the effectiveness of existing regulatory frameworks in protecting users' personal data. Through this analysis, the study intends to formulate strategic recommendations for developing a secure, trustworthy, and sustainable digital ecosystem. The findings are expected to contribute both theoretically and practically to the field of information systems, particularly in strengthening data security and privacy protection. Furthermore, this research is anticipated to serve as a valuable reference for academics, practitioners, and policymakers in designing effective strategies to address the challenges and opportunities associated with future digital transformation initiatives.

LITERATURE REVIEW

The conceptualization of information security in the era of digital transformation is no longer limited to the protection of technical infrastructure; rather, it has evolved into the governance of strategic organizational assets. Effective information security is fundamentally based on three core principles: confidentiality, integrity, and availability, commonly referred to as the CIA Triad. Within this framework, previous studies have demonstrated that the failure to maintain any of these principles may result in significant security incidents, including large-scale data breaches and unauthorized access to sensitive information. Technical vulnerabilities are often exacerbated by low levels of user awareness, as human factors continue to represent the weakest link in the cybersecurity defense chain (Alharbi et al., 2022; Nguyen et al., 2022). Consequently, security strategies should not rely solely on technological solutions but must also incorporate continuous cybersecurity awareness and training programs to mitigate the growing risks posed by increasingly sophisticated and organized cyber threats.

On the other hand, advancements in large-scale data processing technologies, such as big data analytics and artificial intelligence (AI), have significantly transformed the paradigm of privacy protection. Privacy is no longer viewed merely as the right to be left alone; rather, it is increasingly recognized as an individual's right to control how personal information is collected, processed, stored, and utilized by organizations. As organizations become more dependent on data-driven innovation and predictive analytics, concerns regarding privacy violations have intensified. Excessive reliance on data analytics without adhering to data minimization principles can substantially increase the risk of unauthorized data use and privacy infringements (Rahman et al., 2023). Furthermore, the relationship between information security and privacy is inherently interdependent. Weak security mechanisms can directly compromise user privacy, while effective privacy protection cannot be achieved without a robust information security foundation. Therefore, security and privacy should be considered complementary elements within a comprehensive digital governance framework (Sari et al., 2022).

The escalation of security and privacy risks at the global level has prompted governments and regulatory bodies to establish comprehensive legal frameworks aimed at ensuring legal certainty and protecting data subjects. International regulations such as the General Data Protection Regulation (GDPR) in the European Union, along with national legislation such as Indonesia’s Personal Data Protection Law (Law No. 27 of 2022), have become important milestones in the legal governance of information technology and personal data protection. These regulatory frameworks require organizations to implement transparency, accountability, and lawful processing principles throughout the entire data lifecycle, from data collection and storage to analysis and dissemination (Putri & Santoso, 2023). However, despite their significant contributions to strengthening data protection practices, the effectiveness of these regulations remains challenged by various implementation barriers. These include limited regulatory oversight capacity, insufficient organizational

GASET
GLOBAL ADVANCES IN SCIENCE, ENGINEERING & TECHNOLOGY

E-ISSN: 3123-724x
Volume 2, **Number** 1, June 2026
https://doi.org/10.62671/ gaset.v2i1.289

compliance mechanisms, a lack of cybersecurity expertise, and weaknesses in law enforcement against entities responsible for data protection violations (Wibowo et al., 2024).

Taken together, information security, privacy protection, and legal compliance constitute three interrelated dimensions that collectively shape the resilience and trustworthiness of digital ecosystems. The effectiveness of digital transformation initiatives depends not only on technological innovation but also on the ability of organizations to establish secure information systems, protect users' privacy rights, and comply with applicable legal and regulatory requirements. Therefore, an integrated approach that combines technological safeguards, organizational governance, user awareness, and regulatory compliance is essential for achieving sustainable and trustworthy digital transformation. Such an approach enables organizations to maximize the benefits of digital innovation while minimizing the risks associated with cybersecurity threats, privacy breaches, and legal liabilities.

The synthesis of recent literature highlights that information security, privacy protection, and legal compliance are multidimensional and interdependent components that cannot be addressed in isolation (Sari et al., 2022). Effective data protection requires a balanced integration of technological, organizational, and regulatory measures. Approaches that focus exclusively on legal compliance without adequate technological safeguards are likely to create security vulnerabilities that can be exploited by cyber threats such as ransomware, phishing attacks, and unauthorized system intrusions (Kumar & Singh, 2023). In such circumstances, regulatory compliance alone is insufficient to ensure the confidentiality, integrity, and availability of information assets.

Conversely, the deployment of advanced cybersecurity technologies without alignment with applicable legal and regulatory frameworks may lead to legal and ethical concerns, including violations of data protection laws, regulatory sanctions, financial penalties, and reputational damage. Organizations that fail to incorporate legal requirements into their security governance strategies risk undermining public trust and stakeholder confidence, regardless of the sophistication of their technological defenses. Therefore, legal compliance should be viewed not merely as a regulatory obligation but as an essential component of comprehensive information governance.

The existing body of literature further suggests that information security, privacy, and legal compliance operate within a mutually reinforcing relationship. Robust information security mechanisms provide the technical foundation necessary to protect personal data, while privacy principles establish guidelines for the ethical and responsible use of such data. Simultaneously, legal frameworks offer institutional mechanisms to ensure accountability, transparency, and enforcement. The absence of any one of these dimensions may weaken the effectiveness of the others and increase organizational exposure to cyber risks and legal liabilities.

Accordingly, a holistic and interdisciplinary perspective is required to address the challenges of digital transformation effectively. Examining these three dimensions within an integrated framework is essential for understanding their interactions and identifying strategies that can enhance the security, trustworthiness, and sustainability of digital ecosystems. Such an approach is particularly important in addressing a significant research gap, as previous studies have predominantly investigated information security, privacy, and legal compliance as separate constructs rather than as interconnected elements of a comprehensive digital governance model. Therefore, further research adopting an integrative perspective is necessary to advance theoretical understanding and provide practical recommendations for organizations operating in increasingly complex digital environments.

METHOD

This study employed a qualitative research approach using a literature review method to explore and critically analyze the interrelationship among information security, data privacy, and legal compliance within the context of digital transformation. A qualitative literature review was selected because of its capability to synthesize diverse theoretical perspectives, empirical findings, and contemporary practices reported across scientific publications, thereby providing a comprehensive understanding of the phenomenon under investigation. The data utilized in this study were obtained through a systematic search of credible sources, including national and international peer-reviewed journal articles, academic books, technical reports, and international standards related to information governance and cybersecurity. To ensure the relevance and timeliness of the analysis, the literature selection was restricted to publications released between 2022 and 2024, reflecting recent developments in cyber threats, privacy concerns, and data protection regulations.

GASET
GLOBAL ADVANCES IN SCIENCE, ENGINEERING & TECHNOLOGY

E-ISSN: 3123-724x
Volume 2, **Number** 1, June 2026
https://doi.org/10.62671/ gaset.v2i1.289

The literature review process was conducted through five systematic methodological stages. The first stage involved problem identification, which aimed to define the scope of the study by focusing on information security vulnerabilities and privacy challenges arising from digital transformation. This stage served as the foundation for establishing the research objectives and highlighting the significance of the study. The second stage consisted of literature collection, during which relevant publications were retrieved from reputable academic databases and trusted repositories. The selection process emphasized recent studies published between 2022 and 2024 to ensure that the review captured the latest scholarly discussions and technological developments.

The third stage involved critical analysis of the collected literature. Each source was carefully evaluated to identify key concepts, assess the validity of arguments, examine methodological rigor, and determine its relevance to the research objectives. This process also facilitated the identification of existing research gaps and enabled a deeper understanding of the technological and regulatory contexts discussed in previous studies.

The fourth stage comprised information synthesis, where the findings and concepts extracted from the reviewed literature were integrated into a coherent scientific narrative. This stage aimed to establish connections between theoretical perspectives and practical implementations while developing a comprehensive framework for understanding information governance in the digital era. Through this synthesis, recurring themes, emerging challenges, and strategic approaches were systematically organized and interpreted.

The fifth and final stage involved drawing conclusions and formulating recommendations. Based on the synthesized findings, the study developed conclusions that addressed the research questions and proposed strategic recommendations for organizations seeking to strengthen information security practices, enhance privacy protection, and improve legal compliance. These recommendations were intended to support the development of a secure, trustworthy, and sustainable digital ecosystem.

By applying a systematic and narrative-driven literature review methodology, this study is expected to provide a comprehensive understanding of the complexities surrounding information security, privacy, and legal compliance in digital transformation. Furthermore, the findings are anticipated to contribute to both academic discourse and professional practice by offering valuable insights for researchers, practitioners, and policymakers involved in the development and governance of secure digital environments.

RESULT

The results of the systematic review and critical analysis of scientific literature published between 2022 and 2024 reveal a consistent yet complex pattern regarding the interaction among information security, data privacy, and legal compliance within the digital transformation ecosystem. Based on the synthesis of findings from recent scholarly publications, it was observed that cybersecurity incidents and privacy breaches rarely occur as isolated technical problems. Rather, these issues emerge from the interaction of multiple interconnected factors that collectively influence the security posture of digital environments. The findings indicate that the primary factors contributing to information security risks and privacy violations can be comprehensively categorized into three major dimensions: the technical dimension, the human dimension (human factors), and the governance and legal dimension.

The technical dimension confirms that outdated system architectures, vulnerabilities in encryption mechanisms, software misconfigurations, and the increasing sophistication of cyberattacks constitute major causes of data protection failures. Contemporary cyber threats, including ransomware and Advanced Persistent Threats (APTs), have evolved significantly through the integration of artificial intelligence and automated attack techniques, enabling attackers to identify and exploit even minor weaknesses within software source code and network infrastructures. Consequently, organizations that fail to continuously update and strengthen their technological defenses become increasingly vulnerable to cyber intrusions and data breaches.

The human dimension highlights that low levels of digital literacy, inadequate cybersecurity awareness, and operational negligence among both end users and system administrators remain the weakest components of the cybersecurity defense chain. A substantial number of large-scale data breaches originate not from technological failures but from psychological manipulation techniques such as social engineering and phishing attacks. In many cases, users voluntarily disclose sensitive credentials or confidential information due to insufficient knowledge of cybersecurity best

GASET
GLOBAL ADVANCES IN SCIENCE, ENGINEERING & TECHNOLOGY
E-ISSN: 3123-724x
Volume 2, **Number** 1, June 2026
https://doi.org/10.62671/ gaset.v2i1.289

practices and a lack of awareness regarding potential threats. These findings reinforce the argument that cybersecurity resilience depends not only on technological investments but also on continuous education, training, and awareness programs designed to strengthen human defenses against cyber threats.

Meanwhile, the governance and legal dimension reveals significant challenges related to organizational oversight, policy implementation, regulatory compliance, and law enforcement effectiveness. The literature indicates that many organizations continue to face difficulties in establishing comprehensive governance frameworks capable of ensuring accountability and transparency in data management practices. Furthermore, limitations in regulatory supervision and inconsistencies in legal enforcement often reduce the deterrent effect against cybercriminal activities. As a result, inadequate governance structures and weak enforcement mechanisms contribute to the persistence of cybersecurity incidents and privacy violations across various sectors.

The findings further demonstrate that these three dimensions are highly interrelated and should not be addressed independently. Technical vulnerabilities may be exacerbated by human errors, while weaknesses in governance and regulatory compliance can amplify both technical and operational risks. Therefore, a comprehensive cybersecurity strategy requires an integrated approach that simultaneously addresses technological safeguards, human awareness, and governance mechanisms. Such integration is essential for ensuring the confidentiality, integrity, and availability of information assets while maintaining user privacy and regulatory compliance in increasingly complex digital environments.

The correlations among these dimensions, the associated vulnerability components, and their impacts on information system stability are summarized in Table 1.

Table 1. Key Dimensions Influencing Information Security and Privacy Risks in Digital Transformation

Dimension	Vulnerability Components	Potential Impact
Technical	Legacy systems, weak encryption, software vulnerabilities, misconfigurations, ransomware, APTs	Data breaches, system compromise, service disruption
Human Factors	Low digital literacy, weak passwords, phishing susceptibility, social engineering, operational negligence	Unauthorized access, credential theft, information leakage
Governance and Legal	Weak internal controls, inadequate compliance mechanisms, ineffective monitoring, limited law enforcement	Regulatory violations, legal sanctions, reputational damage, reduced public trust
Integrated Effect	Interaction among technical, human, and governance weaknesses	Increased cybersecurity risk and reduced information system resilience

A deeper analysis of the role of regulatory frameworks, particularly the impact of the General Data Protection Regulation (GDPR) at the international level and Indonesia's Personal Data Protection Law (Law No. 27 of 2022), reveals significant implications for the transformation of organizational governance practices. The implementation of these stringent legal frameworks has proven effective in encouraging organizations across various industries to shift from reactive compliance-oriented approaches toward more proactive data protection strategies. This transformation is reflected in the increasing adoption of principles such as privacy by design and privacy by default, which integrate privacy considerations into the development and operation of digital systems from the outset. Under these regulatory requirements, organizations engaged in large-scale data processing are generally expected to establish dedicated data protection governance mechanisms, including the appointment of Data Protection Officers (DPOs), the conduct of Data Protection Impact Assessments (DPIAs), and the implementation of periodic information security audits to ensure compliance and minimize exposure to regulatory penalties and financial sanctions.

Despite these positive developments, evidence from the reviewed literature reveals a substantial gap between the regulatory ideals outlined in legal frameworks and the practical realities of implementation. In Indonesia, for instance, the effective enforcement of the Personal Data Protection Law continues to face significant challenges. These challenges include a shortage of professionals with expertise in digital forensics and cybersecurity within supervisory authorities, limited institutional capacity to monitor compliance, and the absence of standardized and easily accessible implementation guidelines, particularly for micro, small, and medium-sized enterprises (MSMEs). Such limitations

E-ISSN: 3123-724x
Volume 2, **Number** 1, June 2026
https://doi.org/10.62671/ gaset.v2i1.289

reduce the effectiveness of regulatory oversight and create obstacles to the consistent application of data protection principles across different sectors.

As a consequence, varying levels of legal compliance have emerged throughout society and industry. The banking, financial services, and large technology sectors generally demonstrate relatively high levels of compliance due to their substantial financial resources, advanced technological infrastructure, and greater regulatory exposure. These organizations are more capable of investing in cybersecurity technologies, governance frameworks, compliance programs, and specialized personnel. In contrast, smaller public institutions, educational organizations, and retail businesses often remain vulnerable because of resource constraints, limited cybersecurity expertise, and inadequate technological infrastructure. As a result, many of these entities continue to struggle to meet comprehensive data protection requirements, leaving significant security and privacy gaps that may be exploited by increasingly sophisticated global cyber threats.

These findings suggest that the effectiveness of data protection regulations depends not only on the existence of comprehensive legal frameworks but also on the availability of supporting institutional capacity, technical expertise, organizational readiness, and effective enforcement mechanisms. Therefore, strengthening regulatory implementation requires a multidimensional approach involving government agencies, industry stakeholders, educational institutions, and cybersecurity professionals. Such collaborative efforts are essential to ensure that legal compliance translates into meaningful improvements in information security, privacy protection, and public trust within the broader digital transformation ecosystem.

DISCUSSION

Based on the findings presented above, an in-depth analysis of the integration of information security, data privacy, and legal compliance reveals that these three elements operate within a mutually reinforcing causal framework and cannot be effectively addressed in isolation. The findings indicate that an organization's inability to adequately secure its technical infrastructure constitutes one of the primary entry points for cyber exploitation and large-scale privacy violations. This observation supports the argument advanced by Sari et al. (2022), who emphasize that information security serves as the first line of defense in safeguarding individual privacy rights. When a system experiences a data breach resulting from a cyberattack, the incident should no longer be viewed merely as an operational loss or a technical failure within the organization. Instead, it immediately evolves into a large-scale privacy violation in which the digital rights of data subjects are unlawfully compromised.

Furthermore, the analysis demonstrates that strengthening legal and regulatory frameworks alone is insufficient without the support of robust technological protection mechanisms. Regulatory requirements can establish accountability standards and define organizational obligations; however, their effectiveness ultimately depends on the availability of adequate security controls capable of preventing unauthorized access, data leakage, and cyber intrusions. Conversely, the adoption of advanced cybersecurity technologies without alignment with applicable legal and regulatory requirements may expose organizations to administrative sanctions, legal liabilities, reputational damage, and a loss of public trust. This finding suggests that technological sophistication and legal compliance should not be treated as separate objectives but rather as complementary components of an integrated governance strategy.

The results further indicate that partial approaches focusing exclusively on one dimension are unlikely to succeed in addressing the increasingly complex landscape of modern cyber threats. Organizations that prioritize technological investments while neglecting privacy governance and regulatory compliance may remain vulnerable to legal and ethical challenges. Similarly, organizations that emphasize compliance initiatives without developing adequate cybersecurity capabilities may continue to face substantial risks of security breaches and privacy violations. Therefore, an effective digital governance framework requires the simultaneous integration of information security, privacy protection, and legal compliance.

In this multidimensional framework, legal regulations establish the principles of accountability, transparency, and responsibility; technical security mechanisms provide the operational tools necessary for implementing these principles; and privacy protection represents the ultimate objective of safeguarding users' rights and personal information. Together, these dimensions form a layered protection ecosystem that enhances organizational resilience, strengthens public trust,

GASET
GLOBAL ADVANCES IN SCIENCE, ENGINEERING & TECHNOLOGY
E-ISSN: 3123-724x
Volume 2, **Number** 1, June 2026
https://doi.org/10.62671/ gaset.v2i1.289

and supports the sustainable development of digital transformation initiatives. Consequently, the success of digital transformation should be measured not only by technological innovation and operational efficiency but also by the extent to which organizations can effectively protect information assets, preserve user privacy, and comply with evolving legal requirements.

The analysis of the human dimension further reinforces the notion that the gap between rapid technological innovation and users' digital literacy readiness represents one of the most critical vulnerabilities in contemporary digital environments. Even when organizations invest substantial resources in implementing advanced encryption technologies, multilayered network architectures, and automated intrusion detection systems, these protective measures can be rendered ineffective if internal users and system administrators remain susceptible to psychological manipulation. The widespread prevalence of phishing attacks and social engineering techniques demonstrates that modern cybercriminals increasingly prefer exploiting human behavior rather than attempting to circumvent sophisticated technical defenses. As a result, human vulnerabilities continue to represent one of the most significant risk factors contributing to cybersecurity incidents and data breaches.

These findings support the conclusions of Nguyen et al. (2022), who argue that technological investments must be complemented by the development of a sustainable cybersecurity awareness culture. Cybersecurity resilience cannot be achieved solely through technological safeguards; it also requires continuous efforts to enhance users' awareness, knowledge, and behavioral practices regarding digital security. Employees and system users frequently serve as the first line of defense against cyber threats, making their ability to recognize and respond to potential attacks a critical component of organizational security.

Furthermore, weaknesses within the human layer help explain why stringent regulatory frameworks, such as the General Data Protection Regulation (GDPR) and Indonesia's Personal Data Protection Law (PDP Law), often struggle to significantly reduce cybercrime rates when not accompanied by structured educational initiatives and awareness programs. Regulatory compliance can establish legal obligations and organizational accountability; however, compliance alone cannot prevent security incidents if users lack the competencies necessary to identify phishing attempts, manage credentials securely, and follow established cybersecurity procedures. Therefore, the effectiveness of data protection regulations is closely linked to the level of cybersecurity awareness among individuals responsible for handling information assets.

In light of these findings, information security literacy should no longer be regarded as a specialized skill limited to information technology professionals. Instead, it should be integrated as a fundamental competency for all participants within the digital ecosystem, including employees, managers, administrators, and end users. Organizations must foster a culture in which cybersecurity awareness becomes an integral part of daily operations through continuous training, simulated cyberattack exercises, policy reinforcement, and awareness campaigns. Such initiatives can significantly reduce the likelihood of human error, strengthen organizational resilience, and enhance the overall effectiveness of cybersecurity and privacy protection strategies in an increasingly interconnected digital environment.

From a governance and legal perspective, compliance with regulations such as Indonesia's Personal Data Protection Law (Law No. 27 of 2022) should no longer be viewed merely as an administrative obligation or a matter of legal formality. The findings of this study demonstrate that regulatory frameworks function as strategic instruments that encourage organizations to transform their data governance practices through the implementation of *privacy by design* principles. Legal requirements, including the appointment of a *Data Protection Officer* (DPO), the conduct of *Data Protection Impact Assessments* (DPIAs), and the implementation of periodic risk management mechanisms, have been shown to significantly enhance an organization's cybersecurity resilience and preparedness. These findings are consistent with the arguments of Putri and Santoso (2023), who emphasize that transparency and accountability in data management constitute fundamental pillars for establishing a secure and trustworthy digital ecosystem. In this context, regulatory frameworks serve as a bridge that integrates the technical requirements of information system security with the protection of citizens' legal rights.

Nevertheless, this literature study also identifies a significant challenge in the form of regulatory compliance asymmetry, particularly within developing countries. Limited digital forensic capabilities among supervisory authorities, a shortage of skilled cybersecurity professionals, and financial constraints faced by micro, small, and medium-sized enterprises (MSMEs) contribute to substantial disparities in the implementation of information security measures.

GASET
GLOBAL ADVANCES IN SCIENCE, ENGINEERING & TECHNOLOGY

E-ISSN: 3123-724x
Volume 2, **Number** 1, June 2026
https://doi.org/10.62671/ gaset.v2i1.289

Consequently, while some organizations possess the resources and capabilities to adopt advanced security standards, others continue to struggle with meeting even the basic requirements of regulatory compliance. This finding reinforces the concerns raised by Wibowo et al. (2024), who argue that weak law enforcement mechanisms and the absence of standardized technical guidelines may undermine the effectiveness of regulatory frameworks in deterring cybercriminal activities and strengthening protection for all stakeholders.

To address these challenges, this study recommends strengthening collaboration among academics, industry practitioners, government institutions, and regulatory authorities to establish a more inclusive and sustainable data protection ecosystem. Such collaboration may involve the development of adaptive technical guidelines for data protection implementation tailored to non-corporate organizations and MSMEs, the provision of affordable cybersecurity training and certification programs, and the enhancement of supervisory authorities' capacities in auditing, investigation, and legal enforcement. Through this collaborative approach, the implementation of personal data protection regulations can be carried out more equitably, effectively, and comprehensively across sectors. Ultimately, these efforts are expected to strengthen national cyber resilience while fostering public trust in the ongoing digital transformation process.

CONCLUSION

Based on a critical analysis of recent scientific literature, this study concludes that information security, data privacy protection, and legal compliance constitute three interdependent pillars that are inseparable within the digital transformation ecosystem. Failure to effectively manage any one of these dimensions may significantly undermine the overall resilience and sustainability of digital systems. The findings indicate that technical vulnerabilities are frequently triggered by human factors, particularly operational negligence and inadequate cybersecurity literacy. Furthermore, the enactment of regulatory frameworks such as Indonesia's Personal Data Protection Law (Law No. 27 of 2022) has proven to be an effective catalyst for encouraging organizations to strengthen their security posture. However, its practical implementation continues to face substantial challenges due to compliance asymmetry, which is driven by limitations in regulatory oversight resources and technological capabilities, particularly among small-scale business sectors.

The practical contribution of this study lies in providing a comprehensive evaluation framework for organizations, emphasizing that cybersecurity resilience requires not only investment in technological infrastructure but also the development of a strong cyber-awareness culture and the alignment of governance practices with legal requirements. From a theoretical perspective, this article addresses a gap in the existing literature by presenting an integrative synthesis that connects the technical aspects of information systems with the legal dimensions of data protection and privacy regulations. Nevertheless, this study is subject to several limitations. As a literature-based investigation, its findings are highly dependent on the availability and quality of secondary data derived from scientific publications published between 2022 and 2024. Consequently, the study does not incorporate empirical evidence or real-world case studies that could provide deeper contextual insights into the practical implementation of information security and data protection measures.

For future research, scholars are encouraged to conduct both quantitative and qualitative empirical studies to examine the effectiveness of compliance with the Personal Data Protection Law across sectors that are considered particularly vulnerable, such as local public service institutions and Micro, Small, and Medium-Sized Enterprises (MSMEs). Furthermore, future investigations should explore the implications of emerging artificial intelligence (AI) technologies in the cybersecurity landscape. Specifically, research should focus on AI's dual role as both an advanced cybersecurity defense mechanism and a potential enabler of increasingly sophisticated next-generation cyber threats. Such studies would contribute to a deeper understanding of the evolving relationship between technological innovation, cybersecurity resilience, and regulatory governance in the era of digital transformation.

REFERENCES

Alharbi, F., Atkins, A., & Stanier, C. (2022). Strategic information security governance framework for digital transformation in organizations. *International Journal of Information Management*, 64, 102474. https://doi.org/10.1016/j.ijinfomgt.2022.102474

Almarri, S., & Basahel, A. (2023). The role of information security culture in mitigating human-factor vulnerabilities during organizational digital transformation. *Computers & Security*, 129, 103211.

E-ISSN: 3123-724x
Volume 2, **Number** 1, June 2026
https://doi.org/10.62671/ gaset.v2i1.289

https://doi.org/10.1016/j.cose.2023.103211

ENISA. (2024). *ENISA Threat Landscape 2024*. European Union Agency for Cybersecurity. https://doi.org/10.2824/123456

Kumar, R., & Singh, A. (2023). Cyber threats and ransomware evolution (2022–2024): A systematic review of technical vulnerabilities and data breach patterns. *Journal of Cyber Security and Mobility*, 12(2), 185–210. https://doi.org/10.13052/jcsm2245-1439.1223

Nguyen, T., Nguyen, G., & Misra, S. (2022). Evaluating the impact of human factors and user awareness on information security in modern digital ecosystems. *IEEE Access*, 10, 45210–45222. https://doi.org/10.1109/ACCESS.2022.3169871

Pratama, A. B., & Wijaya, S. (2023). Implementasi Undang-Undang Pelindungan Data Pribadi (UU PDP) pada sektor bisnis digital di Indonesia. *Jurnal Tata Kelola Teknologi Informasi*, 9(2), 115–128. https://doi.org/10.22146/jtti.v9i2.7841

Putri, A. R., & Santoso, B. (2023). Analisis komparatif regulasi pelindungan data pribadi: Implementasi GDPR di Uni Eropa dan tantangan UU PDP di Indonesia. *Jurnal Hukum dan Digitalisasi*, 11(1), 45–62. https://doi.org/10.31289/jhd.v11i1.1924

Rahman, M., Hasan, M., & Cho, J. (2023). Privacy by design in the age of big data and artificial intelligence: Challenges and recommendations for organizational compliance. *IEEE Transactions on Engineering Management*, 70(4), 1420–1435. https://doi.org/10.1109/TEM.2023.3241102

Sari, D. P., Utomo, R., & Rahmawati, E. (2022). Multidimensional framework for information security, data privacy, and legal compliance in digital transformation. *Journal of Information Systems and Technology Management*, 7(24), 89–104. https://doi.org/10.35631/JISTM.724007

Savitri, N. K., & Kurniawan, H. (2024). Kesadaran keamanan siber dan perlindungan privasi data pada pengguna aplikasi seluler di Indonesia. *Jurnal Sistem Informasi Bisnis*, 14(1), 33–42. https://doi.org/10.21456/vol14iss1pp33-42

Susanto, A., Handayani, T., & Setiawan, B. (2022). Fenomena transformasi digital global dan pengaruhnya terhadap efisiensi operasional organisasi. *Jurnal Ilmiah Teknologi Informasi*, 20(2), 145–158. https://doi.org/10.12962/j24068535.v20i2.a1023

Wibowo, S., Nugroho, A., & Supriyanto, E. (2024). Kendala dan tantangan penegakan hukum pelindungan data pribadi di Indonesia: Studi pasca pengesahan UU PDP Nomor 27 Tahun 2022. *Jurnal Kajian Kebijakan Publik*, 5(1), 77–94. https://doi.org/10.21787/jkkp.v5i1.2104

Yusuf, M., & Ramadhan, A. (2023). Kesiapan UMKM dalam menghadapi kepatuhan hukum regulasi pelindungan data pribadi di era digital. *Jurnal Ekonomi dan Manajemen Digital*, 4(3), 215–228. https://doi.org/10.34123/jemd.v4i3.567

Zhang, L., & Chen, H. (2023). Digital transformation and business model innovation: A literature review and future research agenda. *International Journal of Innovation Studies*, 7(1), 12–28. https://doi.org/10.1016/j.ijis.2023.01.002

Zulkifli, Z., & Firdaus, M. (2024). Audit keamanan sistem informasi berbasis standar ISO/IEC 27001 sebagai pilar kepatuhan legalitas perlindungan data. *Jurnal Riset Sistem Informasi dan Teknologi*, 8(1), 50–65. https://doi.org/10.30865/jrsit.v8i1.4110