The Indonesian Journal of Computer Science
www.ijcs.net
Volume 14, Issue 2, April 2025
https://doi.org/10.33022/ijcs.v14i2.4637

Investigating Challenges in Information Security Governance Implementation in Key Sectors: A Cross-Country Comparative Analysis

Karisa Saraswati[1], Betty Purwandari[2], Ni Wayan Trisnawaty[3]
karisa.saraswati11@ui.ac.id[1], bettyp@cs.ui.ac.id[2], ni.wayan05@ui.ac.id[3]
[1,2,3] Fakultas Ilmu Komputer, Universitas Indonesia, Jakarta, Indonesia

Article Information

Diterima : 11 Jan 2025
Direvisi : 23 Apr 2025
Disetujui : 30 Apr 2025

Keywords

Information Security Governance (ISG), Challenges in Information Security, Cybersecurity Challenges, Systematic Literature Review (SLR), Risk Management in Information Security

Abstract

The increasing reliance on digital systems has heightened cybersecurity threats, emphasizing the critical need for effective information security governance (ISG). This study examines the challenges faced by Indonesian organizations in implementing ISG and compares them with those encountered in developing and developed countries. Using a systematic literature review (SLR) and expert interviews, this research identifies 34 key challenges in the Indonesian context, categorized into organizational, human, physical, and technological domains. The findings reveal that Indonesian organizations face resource limitations, inadequate leadership support, and low employee awareness, similar to other developing nations. However, Indonesia also experiences unique barriers, such as bureaucratic inefficiencies in government institutions. Comparative analysis shows that developing countries share challenges like cultural resistance and insufficient training, while developed nations grapple with regulatory complexities and integrate security into mature frameworks. The study concludes that while developed countries benefit from better resources, both contexts require cohesive frameworks, strategic alignment, and enhanced training to address ISG challenges effectively. This research provides actionable recommendations for organizations and policymakers to strengthen ISG practices and mitigate cyber risks.

A. Introduction

In today's dynamic and interconnected world, information is critical for organizations. It is fundamental for decision-making, problem-solving, and maintaining competitive advantage. Without accurate and timely information, organizations risk making costly mistakes. Proper management of information not only enhances operational efficiency but also contributes to strategic success. Information systems support these objectives by facilitating specialized processes and analytical tasks. However, despite their potential, improperly handling information—especially without robust security measures—exposes organizations to cyber threats such as data breaches, ransomware attacks, and other malicious activities [1].

An alarming increase in cybersecurity threats has parallelled the expanding reliance on digital systems. According to the Indonesian Cyber Threat Intelligence (CTI) report from the National Cyber and Crypto Agency (BSSN), 347 suspected cyber incidents were reported in 2023, encompassing data leaks, ransomware, web defacement, potential Distributed Denial-of-Service (DDoS) attacks, and insider threats. BSSN further identified 1,674,185 data exposures across 429 organizations, with the government sector accounting for the largest share at 39.78%, followed by the financial (9.86%), ICT (9.63%), and transportation (3.40%) sectors [2]. These incidents highlight the pressing need for effective information security governance (ISG) to safeguard critical assets and maintain organizational resilience.

Cyber incidents can have profound consequences, including reputational damage, financial losses, erosion of customer trust, and operational disruptions [3]. As organizations increasingly recognize the importance of securing their information assets, implementing dedicated ISG frameworks has become essential. ISG defines roles and responsibilities, allocates resources, and establishes accountability mechanisms to successfully implement security strategies, policies, standards, and awareness programs [4].

Organizations strategically design ISG to align security initiatives with their goals, foster a security-conscious culture, and optimize resource allocation [5]. Its primary objective is to protect information systems and stakeholders from risks related to breaches of confidentiality, integrity, and availability [6]. Despite the availability of internationally recognized frameworks like ISO/IEC 27001 and COBIT 5, many organizations face significant challenges in integrating these practices into their operations [7],[8]. Addressing these challenges is crucial for ensuring organizations remain resilient in an era of increasing cyber threats.

"Organizations can use various international and national standards to ensure that their ISG is consistent with their business strategy [7]. These standards include the ISO/IEC 27000 series, which includes ISO/IEC 27001, ISO/IEC 27002, and others. The COBIT 5 standard also contains provisions regarding information technology governance and security [7]. BSSN has also developed an ISG framework in Indonesia, the Information Security Index (KAMI). Organizations can use this tool to assess and evaluate their readiness for implementing information security based on the SNI ISO/IEC 27001 criteria [8].

Several previous studies have examined the implementation of information security governance. For example, researchers conducted a study in an

organization in Malaysia and found that a lack of awareness of the importance of information security policies and integration into organizational systems were problems in implementing ISG [9]. In addition, a study of state-owned banks in India found that the lack of implementation and monitoring of their information security policies resulted in ineffective ISG at these banks [10].

The widespread implementation of ISG has introduced diverse challenges for organizations worldwide, potentially impacting their effectiveness and success. Despite this, comprehensive comparative studies exploring how these challenges differ across national contexts—particularly between developing and developed countries—remain limited. This study seeks to identify Indonesian organizations' challenges in implementing ISG and compare them with those encountered in developing and developed nations.

Based on the above background, this study addressed three research questions to meet its objectives. First (RQ1), what challenges do Indonesian organizations face in implementing information security? Second (RQ2), how are the challenges in Indonesia compared with other developing countries? Third (RQ3), how are the challenges in developing countries compared with those in developed countries?

This study aims to contribute in two significant ways. First, it gives organizations insights to enhance their ISG practices. Second, it offers a framework for organizations to adapt their governance strategies better to suit their specific national contexts while maximizing the global effectiveness of ISG methodologies.

B. Research Method

This research is desk-based research, which focuses on collecting and analyzing data from relevant secondary sources. This approach aims to summarize and interpret academic literature and previous research related to information security governance. In addition, this research also involves collecting primary data through interviews with two ISG experts, thereby providing an additional dimension to understand the challenges organizations face in Indonesia. The interviews with the experts discuss the data extraction result from a systematic literature review and validate identified challenges. The study based the literature review on a comprehensive research database from Universitas Indonesia, Google Scholar, and IEEE. The three databases were chosen because they have various selections of research on how ISG is implemented in Indonesia. This research aims to identify challenges in implementing ISG in Indonesia, compare challenges in Indonesia and other countries, and give practical and strategic recommendations to help organizations face challenges.

Figure 1 illustrates the research stages. Initially, identifying the research objective leads to establishing research questions. These questions will then guide the keywords to search for research reports in ISG implementations. In step three, this study omitted studies deemed less relevant. Afterward, in step four, the challenges related to ISG implementation in Indonesia were extracted from the selected studies. It concentrated on 34 challenges, organized into four domains identified using open coding. Steps 1 to 4 are adopted from Kitchenham's SLR method, where steps 1 and 2 can be categorized as the planning stage where the SLR needs are identified and the review protocol, which defines the keywords for

the literature search, is built; step 3 is the implementation stage. In this stage, the problem is empirically searched according to the defined review protocol, followed by data extraction and synthesis. Step 4 is the reporting stage, which results in a review form being created [11].

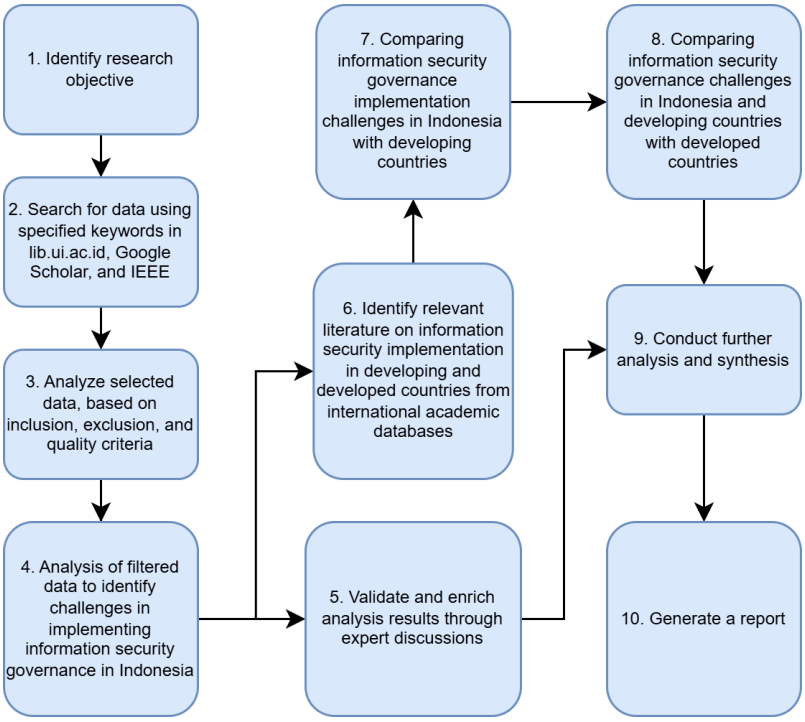

Figure 1. Research Stages

In step five, this study interviewed two information security experts in Indonesia to validate and enhance the identification of the challenges. The sixth phase expanded the scope by searching international studies to identify scholarly works on implementing ISG in developing and developed countries. Subsequently, in steps seven and eight, the challenges identified in steps four and five were compared to those discovered in step six. Step nine involved synthesizing the challenges faced in implementing ISG in Indonesia with those from other developing and developed countries. In step ten, this study consolidated the insights into a detailed report.

This study has several phases of data collection. Steps two and three of Figure 2 illustrate the initial data collection phase. Step two represents the search process for relevant studies using keywords in three databases: lib.ui.ac.id (Universitas Indonesia's research database), Google Scholar, and IEEE. ISG implementation is not a typical research topic for students of Universitas Indonesia. Therefore, this study is widening the source to capture studies related to implementing ISG in Indonesia, providing valuable insight into the process within the country.

The keywords used in the search process include Information Security Management Systems (ISMS), ISG in Indonesia, challenges in information security governance, ISMS challenges in Indonesia, and ISMS implementation evaluation in

Indonesia. Identifying and creating suitable keywords is crucial for finding relevant literature on the research topic.

In the next step, this study applied the identified criteria. One of these criteria was to set the period for relevant studies, which this study chose between 2019 and 2024. This study also established quality assurance criteria to ensure relevance to the research questions. This study included studies that met all the criteria in the research. The quality assurance criteria are as follows:

1 QA1: Does the research include relevant studies regarding implementing information security governance?
2 QA2: Are the research data presented adequately?
3 QA3: Were the inclusion criteria met in this study?

During the initial keyword search in three databases, we found 127 studies. After applying the inclusion and exclusion criteria, we retained 72 studies. Next, 60 studies remained after eliminating duplicate data. Subsequently, quality control measures were applied, resulting in 40 studies on ISG implementation, as illustrated in Figure 2.

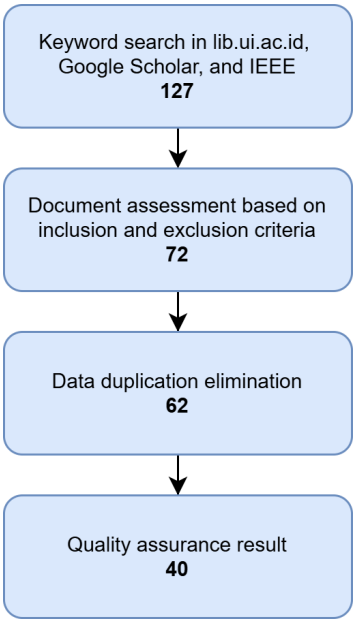

Figure 2. Document Selection Process for Literature Review

Figure 2 shows the second data collection in step five. The process involved interviews with three experts in ISG implementation in Indonesia. These interviews aimed to validate and further explore the challenges identified earlier in step four, as illustrated in Figure 3. Each expert has at least five years of experience implementing information security governance. Expert A, with almost eleven years of experience, served as a Vice President of an Indonesian digital identity company. Expert B has 5 years of experience and works as a Junior IT Security Specialist at an Indonesian government institution. The interviews provided valuable insights into the challenges of implementing information

security governance, which were analyzed through open coding to uncover recurring themes.

The third data collection process in step six of Figure 2 involved a systematic literature review (SLR) to identify relevant papers on ISG implementation in developed and developing countries. This review used the lib.ui.ac.id database and Google Scholar. Keywords such as "Information Security Governance Challenges," "Obstacle in Information Security Governance," "ISMS Challenges," and "ISMS Obstacles" were utilized.

This study identified fourteen papers that cover challenges in implementing information security governance. Developed countries represented the UK, USA, Australia, Sweden, China, and Europe, while Saudi Arabia, India, Portugal, Zanzibar, Ghana, Turkey, and various African countries represented developing nations. The selected papers underwent a detailed review to analyze their topics, research questions, methodologies, and findings. Key insights and conclusions were summarized, revealing seven studies focusing on implementation in developing countries [12], [13], [14]–[18], and six addressing developed countries [19]–[24].

C. Result and Discussion

The extracted data underwent analysis through content analysis methods [25] and open coding [26], which facilitated the identification of key themes and patterns. This systematic approach provided a framework for categorizing the findings, enabling the synthesis of reports and conclusions to address the research question outlined below.

1. RQ1: What challenges do Indonesian organizations face in implementing information security?

The data extracted from the SLR identified 34 challenges faced by organizations in Indonesia. Figure 3 illustrates the distribution of these challenges across different organizational sectors, while Table I categorizes them into organizational, people-related, physical, and technical domains according to their common characteristics. The details are as follows.

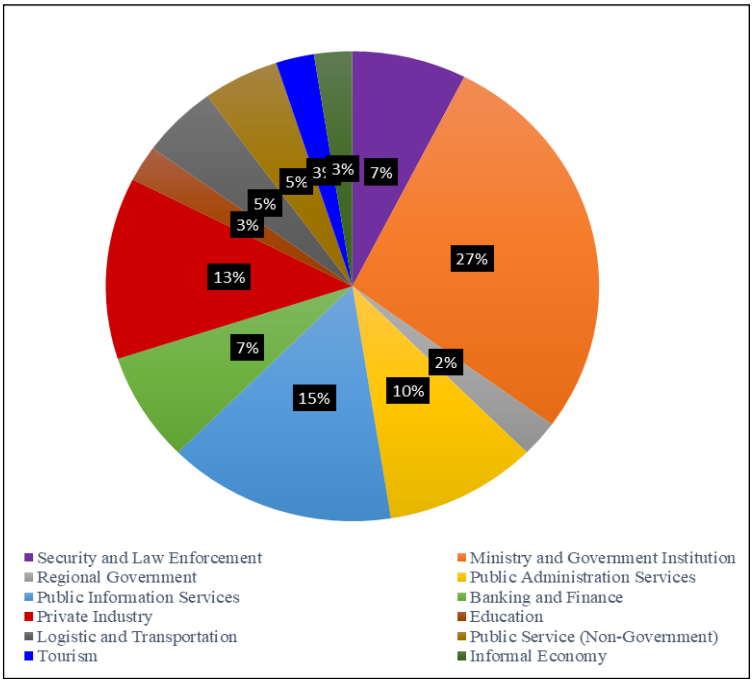

Figure 3. Challenges Distribution in Different Sectors

a. Organizational

Organizational challenges are related to organizational structure, policies, and operational processes. Factors related to coordination, management, and company policies can generally become obstacles from an organizational perspective. Based on the challenges identified in this research, the organizational domain has several sub-themes with details as follows.

1) Information Security Governance (ISG) and Policy

This sub-theme highlights the lack of security investment, unprioritized information security controls implementation, inadequate implementation of information security standards, imperfect information security policy implementation, inadequate information security documentation, and the sustainability of information security standard implementation is still insufficient. These challenges often occur due to gaps and poor integration between information security and organizational strategies [27], [28] . Expert A emphasized that this could happen due to limited support from management, which undermines the planning and prioritization of security investments. Meanwhile, Expert B highlights that suboptimal risk management leads to inadequate investment planning, as it fails to address evolving threats effectively.

2) Framework Integration

The challenges in integrating frameworks for ISG include low adoption of established standards (e.g., ISO/IEC 27001), particularly in government institutions, and unstructured or partial implementation in many organizations, leading to inconsistencies in governance. Policies often operate in isolation, lacking

integration with broader organizational strategies and regulatory goals, creating gaps in alignment and compliance [29], [30].

Additionally, overlapping and ambiguous regulations, such as conflicting domestic laws and unclear synchronization with international standards, further complicate effective framework adoption. These issues underscore the need for clear guidance and cohesive framework integration. Expert A highlights that poor employee awareness and inadequate training contribute to unstructured frameworks, often implemented only in specific departments rather than organization-wide. As for the implementation in government institutions, Expert B emphasized that inadequate adoption of frameworks in government institutions due to poor compliance monitoring and lack of evaluations, leaving weaknesses unaddressed. Additionally, unclear regulations complicate compliance, creating external challenges for organizations to address.

3) Evaluation and Readiness Assessment

The lack of evaluation and readiness assessment in implementing ISG arises from occasional and ad-hoc evaluation practices, insufficient documentation, low governance maturity, weak compliance with standards, and poor readiness for national and international frameworks. Low management awareness, prioritization, and insufficient resources compound these challenges and unsupportive organizational structures [27][30][31][32]. Experts A and B agreed that incomplete and unstructured documentation creates gaps between implementation and compliance, while uneven employee understanding contributes to low governance maturity. Weak adherence to standards and limited focus on security readiness hinder effective governance.

Table 1. Distribution of Information Security Areas by Domain and Subtheme

Domain	Subtheme	Subtheme Percentage	Domain Percentage
Organizational	Information Security Governance and Policy	24.49%	61.90%
	Framework Integration	10.20%	
	Evaluation and Readiness Assessment	27.21%	
People	Competency and Training	8.84%	24.49%
	Information Security Culture	25.65%	
Physical	Physical Environment Security	2.04%	2.04%
Technological	Infrastructure and Technology	2.04%	11.56%
	Technology Risk Management	9.52%	
Organizational	Information Security Governance and Policy	24.49%	61.90%
	Framework Integration	10.20%	
	Evaluation and Readiness Assessment	27.21%	
People	Competency and Training	8.84%	24.49%
	Information Security Culture	25.65%	
Physical	Physical Environment Security	2.04%	2.04%
Technological	Infrastructure and Technology	2.04%	11.56%
	Technology Risk Management	9.52%	

b. People

People-related challenges in implementing ISG include insufficient training, resistance to change, and low employee motivation and awareness. These issues arise from inadequate skills development and a weak security culture characterized by inconsistent organizational attitudes and behaviors. Based on the challenges identified in this research, the organizational domain has several sub-themes with details as follows.

1) Competency and Training

Many organizations face gaps in strategic and technical understanding, with employees unable to align organizational needs with relevant security controls or respond effectively to evolving threats. Inconsistent implementation of security frameworks, such as ISO/IEC 27001, and limited knowledge of key domains like risk management and asset governance worsen these issues [33]. Additionally, a lack of regular training, skill development, and technical guidance prevents employees from effectively managing risks and adopting security governance frameworks [34]. Expert A emphasized that inadequate training and skill development programs directly contribute to employees' lack of competence in handling security governance tasks. Additionally, the lack of employee competency in implementing ISG comes from insufficient training. This condition leads to employees being unaware of the importance of information security and feeling confused about how to implement it effectively.

2) Information Security Culture

This sub-theme highlights low employee awareness, resistance to change, and operational priorities often overshadow security measures. Employees frequently lack training and understanding of safeguarding information, leading to non-compliance with security policies. Resistance to new controls arises when they are perceived as burdensome, compounded by weak management emphasis on fostering a security-oriented culture. Poorly defined roles and insufficient organizational structures hinder implementation, while limited human resources and high implementation costs strain efforts, especially in smaller organizations [35]

These challenges arise from low employee awareness, as Expert A and Expert B noted, due to insufficient management support and traditional work practices. Expert A highlighted that resistance to change is linked to poor teamwork, whilst Expert B emphasized that bureaucratic processes in government institutions hinder the information security culture. Experts A and B agreed that unclear roles, inadequate staffing, and insufficient organizational structures result from budget constraints and a lack of management understanding. Additionally, high implementation costs hinder resource allocation for security governance, highlighting the need for more substantial management commitment, training, and resource investment.

c. Physical

The analysis of ISG challenges in the physical domain focuses on securing physical assets, including facilities, hardware, access control, and infrastructure, to

protect information confidentiality, integrity, and availability. Common challenges include weaknesses in physical access control, poor infrastructure maintenance, and environmental threats like natural disasters.

1) Physical Environment Security

Physical environment security poses significant challenges in implementing ISG due to inadequate facilities, infrastructure, and environmental risks. Organizations often face issues like weak physical access controls, lack of secure data centers, incomplete deployment of critical tools such as firewalls and encryption technologies, and absence of integrated monitoring systems. Additionally, poor maintenance of physical infrastructure and vulnerability to environmental threats, such as natural disasters, further hinder the adequate protection of information assets [36][37]. Expert A emphasized that management's level of support significantly influences the availability and quality of facilities for information security governance.

d. Technological

The analysis of challenges in ISG within the technological domain focuses on evaluating IT infrastructure, security software, network systems, and supporting technologies. Key challenges include misalignment between technology and business needs, cyberattack vulnerabilities, limited system integration, and lack of software updates.

1) Infrastructure and Technology

Infrastructure and technology challenges in implementing ISG come from vulnerabilities in infrastructure management and data centers. Common issues include frequent server downtime, API integration problems, and website breaches, which expose systems to data theft and fraud, undermining public trust. Data centers often face threats due to outdated hardware [38], lack of standardized incident response procedures, and insufficient security measures, such as biometric access controls and integrated CCTV systems

These weaknesses compromise the confidentiality, integrity, and availability of information, leaving systems vulnerable to internal and external threats. The cause of infrastructure challenges in implementing ISG lies in inadequate organizational structures and limited resources. According to Expert B, insufficient organizational resources hinder the proper allocation of responsibilities, making it challenging to implement necessary controls to address vulnerabilities in infrastructure and data centers.

2) Technology Risk Management

Technology risk management presents significant challenges in implementing ISG due to vulnerabilities in infrastructure, outdated systems, and inadequate incident response procedures. Limited resources and insufficient integration of security controls, such as biometric access and monitoring systems, worsen risks. These challenges are often compounded by a lack of standardized frameworks for addressing cyber threats, inadequate allocation of responsibilities, and reactive approaches to risk mitigation, leaving organizations vulnerable to internal and external threats [31].

Expert B highlighted that unclear identification and mitigation of risks, coupled with insufficient budgets for information security, hinder optimal risk management. Additionally, Expert A emphasized the need for strong management support to provide explicit directives for improving information security. These issues underscore the importance of clear leadership, sufficient funding, and robust risk management practices.

2. RQ2: How are the challenges in Indonesia compared with other developing countries?

This research identified seven papers [12], [13], [14]–[18] on ISG implementation from lib.ui,ac.id, and Google Scholar. This study then mapped common challenges to those identified in the SLR.

a. Lack of Strategic Alignment

In Indonesia, organizations tend to find difficulties in aligning ISG with organizational strategies. The lack of strategic alignment in Saudi Arabia arises from insufficient leadership involvement, unclear processes, and weak risk management frameworks [12]. In Turkey, fragmented ISG efforts come from poor prioritization of IT security and limited integration with business objectives [18].

b. Inadequate Risk Management

In Indonesia, these challenges are often compounded by a lack of standardized frameworks for addressing cyber threats, inadequate allocation of responsibilities, and reactive approaches to risk mitigation, leaving organizations vulnerable to internal and external threats. In Portugal, small and medium-sized enterprises (SMEs) face challenges due to limited resources, insufficient cybersecurity awareness, and reliance on outdated technology, which undermines their ability to manage risks effectively [15]. For organizations in Ghana, inadequate risk management comes from the absence of standardized frameworks and limited integration of risk mitigation strategies within organizational processes [17].

c. Cultural Barriers

In Indonesia, precisely in government institutions, the bureaucracy is still high, which hinders the practice of information security governance. In Zanzibar, misalignment between external frameworks and local practices leads to resistance and ineffective adoption [16]. Like Saudi Arabia, hierarchical structures, limited collaboration, low-security awareness, and insufficient training weaken governance efforts [13].

d. Limited Resources and Infrastructure

In Indonesia, some organizations still experience a lack of resource allocation for information security governance. Experts believe that lack of management support and budget limitations are the leading causes of lack of resource allocation. Zanzibar and Saudi Arabia have also experienced similar issues. However, Zanzibar's barriers are more deeply rooted in financial constraints and cultural misalignments, which hinder the adoption of effective frameworks [16]. Saudi Arabia, on the other hand, struggles with inefficiencies in resource utilization

and systemic gaps in infrastructure modernization despite better financial capabilities [13].

e. Lack of Leadership Support

In Indonesia, a lack of leadership support is considered one of the main challenges that result in many obstacles to implementing information security governance. Experts believe that lacking leadership support arises from management's insufficient knowledge of the importance of information security. In Saudi Arabia, organizations consider these challenges a leading cause of misalignment with organizational objectives, unclear roles, and insufficient risk prioritization [12].

f. Deficient Policies and Procedures

Indonesia faces inadequate and insufficient information security documentation, creating gaps between implementation and compliance. Saudi Arabia and Turkey also face challenges with deficient policies and procedures in implementing information security governance, though the root causes and manifestations differ. Saudi organizations grapple with strategic misalignment and procedural inadequacies at a systemic level [12], while Turkish SMEs struggle with a lack of structured implementation and low compliance awareness, compounded by resource constraints [18].

g. Insufficient Training and Awareness

In Indonesia, insufficient skill development, such as training and awareness, leaves employees unaware of information security's importance and confused about its implementation, which weakens governance effectiveness. Other than Indonesia, Saudi Arabia and Ghana face the same issue. Both countries face challenges due to insufficient training and awareness, primarily driven by inadequate leadership focus and resource allocation. At the same time, Saudi Arabia's issue highlights the lack of systematic training programs [12]. Ghana's challenge underscores resource constraints and a failure to integrate security measures with broader organizational goals [17].

3. RQ3: How are the challenges in developing countries compared with those in developed countries?

This study reviewed six papers [18]–[23] on ISG implementation sourced from lib.ui.ac.id and Google Scholar, and the everyday challenges were subsequently aligned with those identified through the systematic literature review (SLR).

a. Cultural and organizational goals alignment

Organizations in developing countries struggle to align ISG to organizational strategies due to leadership gaps, unclear processes, weak risk management, and poor IT security prioritization. This study found that in developed countries such as China, Europe, the USA, and Sweden, cultural factors and national norms significantly influence the adoption and implementation of ISG practices. The

differences in organizational hierarchy and cultural attitudes toward collaboration affect the security practices in those four countries [22][19].

b. Complexity of regulatory compliances

In developing countries, not all organizations are facing these challenges. Indonesia faces overlapping and ambiguous regulations, including conflicting domestic laws and unclear alignment with international standards, highlighting the need for clear guidance and cohesive framework integration. While in developed countries, especially Australia, China, and Europe, the fragmented legal and regulatory frameworks across countries make it challenging for organizations to comply with a unified set of standards. This complexity increases the burden of maintaining compliance with multiple overlapping requirements [23][22].

c. Human factor challenges

Developing countries struggle with adequate ISG due to human factors such as insufficient training and awareness, driven by inadequate leadership focus, resource allocation, and a lack of systematic programs. Developed countries such as the USA, Sweden, and the UK face similar challenges in implementing information security governance. Ensuring compliance and effective governance in those countries are hindered by human-related challenges, including lack of awareness, insufficient training, and resistance to policy enforcement [19]–[21], [24].

d. Resource allocation and Expertise

Developing countries face inadequate resource allocation challenges due to budget constraints, cultural barriers, and inefficient resource utilization. Developed countries like China and Europe struggle to allocate sufficient resources, and a lack of internal expertise hinders them from implementing effective governance frameworks like ISO 27001, where they require significant investment in financial resources and skilled personnel [22].

D. Conclusion

This study provides a comprehensive analysis of the challenges faced by Indonesian organizations in implementing ISG. These challenges, including low adoption and incomplete implementation of frameworks like ISO/IEC 27001, insufficient training, and bureaucratic inefficiencies, hinder the development of robust security practices. Additionally, regulatory ambiguities caused by conflicting domestic laws and unclear synchronization with international standards further complicate governance efforts.

By comparing Indonesia's challenges with those of other developing and developed countries, this research offers unique insights into the global landscape of ISG. While Indonesia shares common issues with other developing nations, such as limited resources and inadequate training programs, its bureaucratic inefficiencies and low-security maturity set it apart. Conversely, despite having more substantial resources and established governance frameworks, developed countries encounter challenges in maintaining compliance with overlapping regulations and integrating security practices into mature governance structures.

This study contributes significantly to understanding ISG implementation in Indonesia by providing a structured framework for analyzing challenges and identifying practical strategies. The findings highlight policymakers' need to streamline regulations, foster leadership engagement, and increase budget allocations for ISG initiatives. For organizations, the study emphasizes the importance of investing in employee training, cultivating a security-conscious culture, and adopting internationally recognized frameworks with localized adaptations. Furthermore, the research underscores the need for stakeholder collaboration to align ISG practices with organizational goals and regulatory requirements.

Strengthening ISG practices in Indonesia is essential to improving cybersecurity resilience and addressing the growing complexity of global digital threats. By implementing cohesive frameworks and fostering strategic alignment, Indonesian organizations can better navigate the challenges of information security governance and enhance their ability to safeguard critical assets.

E. References

[1] Z. Hamdi, A. Anir Norman, N. Nuha Abdul Molok, and F. Hassandoust, "A Comparative Review of ISMS Implementation Based on ISO 27000 Series in Organizations of Different Business Sectors," *J. Phys. Conf. Ser.*, vol. 1339, no. 1, 2019, doi: 10.1088/1742-6596/1339/1/012103.

[2] BSSN, "Lanskap Keamanan Siber Indonesia," no. 70, 2024, [Online]. Available: https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf.

[3] D. Achmadi, Y. Suryanto, and K. Ramli, "On Developing Information Security Management System (ISMS) Framework for ISO 27001-based Data Center," *2018 Int. Work. Big Data Inf. Secur. IWBIS 2018*, pp. 149–157, 2018, doi: 10.1109/IWBIS.2018.8471700.

[4] J. J. Korhonen, K. Hiekkanen, and J. Mykkänen, "Information security governance," *Strateg. Pract. Approaches Inf. Secur. Gov. Technol. Appl. Solut.*, no. January 2012, pp. 53–66, 2012, doi: 10.4018/978-1-4666-0197-0.ch004.

[5] G. Alberto, D. O. Alves, L. Fernando, C. Carmo, A. Cristina, and R. Dutra, "Enterprise Security Governance," *Inf. Secur.*, vol. 00, no. C, pp. 71–80, 2006.

[6] G. S. Antoniou, "A Framework for the Governance of Information Security: Can it be Used in an Organization," *Conf. Proc. - IEEE SOUTHEASTCON*, vol. 2018-April, pp. 1–30, 2018, doi: 10.1109/SECON.2018.8479032.

[7] S. M. Alenazy, R. M. Alenazy, and M. Ishaque, "Governance of Information Security and Its Role in Reducing the Risk of Electronic Accounting Information System," *1st Int. Conf. Adv. Innov. Smart City, ICAISC 2023 - Proc.*, pp. 1–5, 2023, doi: 10.1109/ICAISC56366.2023.10084976.

[8] L. D. A. Jelita, M. N. Al Azam, and A. Nugroho, "Evaluasi Keamanan Teknologi Informasi Menggunakan Indeks Keamanan Informasi 5.0 dan ISO/EIC 27001:2022," *J. SAINTEKOM*, vol. 14, no. 1, pp. 84–94, 2024, doi: 10.33020/saintekom.v14i1.623.

[9] M. S. Mir, S. Wani, and J. Ibrahim, "Critical information security challenges: An appraisal," *2013 5th Int. Conf. Inf. Commun. Technol. Muslim World, ICT4M 2013*, pp. 1–4, 2013, doi: 10.1109/ICT4M.2013.6518890.

[10] H. Diwakar and A. Naik, "Investigation of information security management practices in Indian pubic sector banks," *Proc. - 8th IEEE Int. Conf. Comput. Inf. Technol. Work. CIT Work. 2008*, pp. 276–281, 2008, doi: 10.1109/CIT.2008.Workshops.115.

[11] B. Purwandari, M. A. Hermawan Sutoyo, M. Mishbah, and M. F. Dzulfikar, "Gamification in e-Govemment: A Systematic Literature Review," in *2019 Fourth International Conference on Informatics and Computing (ICIC)*, 2019, pp. 1–5, doi: 10.1109/ICIC47613.2019.8985769.

[12] M. A. Alnatheer, "Understanding and Measuring Information Security Culture in Developing Countries : Case of Saudi Arabia," *Comput. Syst. Inf. Technol.*, vol. 9, no. 14, pp. 897–912, 2012.

[13] A. Abu-Musa, "Information security governance in Saudi organizations: An empirical study," *Inf. Manag. Comput. Secur.*, vol. 18, no. 4, pp. 226–276, 2010, doi: 10.1108/09685221011079180.

[14] H. Malhotra, R. Bhargava, and M. Dave, "Challenges related to information security and its implications for evolving e-government structures: A comparative study between India and African countries," *Proc. Int. Conf. Inven. Comput. Informatics, ICICI 2017*, no. Icici, pp. 30–35, 2018, doi: 10.1109/ICICI.2017.8365370.

[15] Mário Antunes, Marisa Maximiano, Ricardo Gomes, and Daniel Pinto, "Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal," *J. CyberSecurity Priv.*, pp. 219–238, 2021.

[16] H. K. Shaaban, "Enhancing the Governance of Information Security in Developing Countries: The Case of Zanzibar," *PhD Thesis*, p. 2014, 2014.

[17] W. Yaokumah, "Information security governance implementation within Ghanaian industry sectors an empirical study," *Inf. Manag. Comput. Secur.*, vol. 22, no. 3, pp. 235–250, 2014, doi: 10.1108/IMCS-06-2013-0044.

[18] E. Yeniman Yildirim, G. Akalp, S. Aytac, and N. Bayram, "Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey," *Int. J. Inf. Manage.*, vol. 31, no. 4, pp. 360–365, 2011, doi: 10.1016/j.ijinfomgt.2010.10.006.

[19] W. Rocha Flores, E. Antonsen, and M. Ekstedt, "Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture," *Comput. Secur.*, vol. 43, pp. 90–110, 2014, doi: 10.1016/j.cose.2014.03.004.

[20] E. Lomas, "Information governance: Information security and access within a UK context," *Rec. Manag. J.*, vol. 20, no. 2, pp. 182–198, 2010, doi: 10.1108/09565691011064322.

[21] H. Fulford and N. F. Doherty, "The application of information security policies in large UK-based organizations: An exploratory investigation," *Inf. Manag. Comput. Secur.*, vol. 11, no. 2–3, pp. 106–114, 2003, doi: 10.1108/09685220310480381.

[22] R. M. van Wessel, X. Yang, and H. J. de Vries, "Implementing international standards for information security management in China and Europe: A comparative multi-case study," *Technol. Anal. Strateg. Manag.*, vol. 23, no. 8, pp. 865–879, 2011, doi: 10.1080/09537325.2011.604155.

[23] M. Burdon, J. Siganto, and L. Coles-Kemp, "The regulatory challenges of

Australian information security practice," *Comput. Law Secur. Rev.*, vol. 32, no. 4, pp. 623–633, 2016, doi: 10.1016/j.clsr.2016.05.004.
[24] A. C. Johnston and R. Hale, "Improved security through information security governance," *Commun. ACM*, vol. 52, no. 1, pp. 126–129, 2009, doi: 10.1145/1435417.1435446.
[25] M. Vaismoradi, H. Turunen, and T. Bondas, "Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study," *Nurs. Heal. Sci.*, vol. 15, no. 3, pp. 398–405, 2013, doi: 10.1111/nhs.12048.
[26] J. M. Corbin and A. Strauss, "Grounded theory research: Procedures, canons, and evaluative criteria," *Qual. Sociol.*, vol. 13, no. 1, pp. 3–21, 1990, doi: 10.1007/BF00988593.
[27] B. Ashari, "Information Security Governance and Management Capability Assessment: A Lesson Learned from Directorate General of Taxes," *J. Penelit. Pos dan Inform.*, vol. 10, no. 1, p. 15, 2020, doi: 10.17933/jppi.2020.100102.
[28] S. R. Musyarofah and R. Bisma, "Analisis kesenjangan sistem manajemen keamanan informasi (SMKI) sebagai persiapan sertifikasi ISO/IEC 27001:2013 pada institusi pemerintah," *Teknologi*, vol. 11, no. 1, pp. 1–15, 2021, doi: 10.26594/teknologi.v11i1.2152.
[29] R. A. P. P. Gala, R. Sengkey, and C. Punusingon, "Analisis Keamanan Informasi Pemerintah Kabupaten Minahasa Tenggara Menggunakan Indeks KAMI," *J. Tek. Inform.*, vol. 15, no. 3, pp. 189–198, 2020, [Online]. Available: https://ejournal.unsrat.ac.id/index.php/informatika/article/view/31597.
[30] F. M. Kaaffah, Darwan, B. Subaeki, A. B. A. Rahman, K. Manaf, and H. A. Sukardi, "The Information Security Readiness in Indonesian Government Institution: A systematic Literature Review," *Proceeding 2023 17th Int. Conf. Telecommun. Syst. Serv. Appl. TSSA 2023*, pp. 1–4, 2023, doi: 10.1109/TSSA59948.2023.10366969.
[31] F. Wijayanti, D. I. Sensuse, A. A. Putera, and A. Syahrizal, "Assessment of Information Security Management System: A Case Study of Data Recovery Center in Ministry XYZ," *2020 3rd Int. Conf. Comput. Informatics Eng. IC2IE 2020*, pp. 393–398, 2020, doi: 10.1109/IC2IE50715.2020.9274574.
[32] F. T. Ui, "Pengembangan Kerangka ..., Ade Wahyu Kurniawan, FT UI, 2023," 2023.
[33] V. S. Kasma, S. Sutikno, and K. Surendro, "Design of e-Government Security Governance System Using COBIT 2019: (Trial Implementation in Badan XYZ)," *Proceeding - 2019 Int. Conf. ICT Smart Soc. Innov. Transform. Towar. Smart Reg. ICISS 2019*, vol. 2019, 2019, doi: 10.1109/ICISS48059.2019.8969808.
[34] F. I. A. Ui, "Evaluasi sistem ..., Tri Agus Saputra, FIA UI, 2021," 2021.
[35] R. Sinaga and F. Taan, "Penerapan ISO/IEC 27001:2022 dalam Tata Kelola Keamanan Sistem Informasi: Evaluasi Proses dan Kendala," *Nuansa Inform.*, vol. 18, no. 2, pp. 46–54, 2024, doi: 10.25134/ilkom.v18i2.205.
[36] N. Qodarsih, "Information Security Evaluation Using the Information Security Index: A Case Study in Indonesia," *2022 5th Int. Semin. Res. Inf. Technol. Intell. Syst. ISRITI 2022*, pp. 570–575, 2022, doi: 10.1109/ISRITI56927.2022.10052961.
[37] J. S. Suroso, T. H. Hwa, R. Syafaat, Saddam, F. A. Pasaribu, and S. Mujiatun,

"Assessing an Information Security Governance Using IPPF in Multi-Finance Company," *Proc. 2019 Int. Conf. Inf. Manag. Technol. ICIMTech 2019*, vol. 1, no. August, pp. 596–601, 2019, doi: 10.1109/ICIMTech.2019.8843733.

[38] ADELIA TALITHA NUR LAILY, "Analisis Penerapan Standar Iso 27001:2013 Untuk Scale Up Business Pada Perusahaan Startup Delman.Io," 2023, [Online]. Available: https://lib.ui.ac.id/.