DESIGN AND VALIDATION OF AN INFORMATION SECURITY INDEX MODEL FOR ENHANCING E-GOVERNMENT IN INDONESIA

FAIZ MUQORRIR KAAFFAH

ASIA e UNIVERSITY

2025

DESIGN AND VALIDATION OF AN INFORMATION SECURITY INDEX MODEL FOR ENHANCING E-GOVERNMENT IN INDONESIA

FAIZ MUQORRIR KAAFFAH

A Thesis Submitted to Asia e University in
Fulfilment of the Requirements for the
Degree of Doctor of Philosophy

June 2025

ABSTRACT

The absence of a standardized, measurable, and contextually relevant model for assessing information security maturity in Indonesian e-government institutions hinders effective evaluation and planning. This study aims to develop and validate an Information Security Index model tailored to the Indonesian e-government context. As information technology becomes more integral to public services, ensuring information security is essential for maintaining public trust and safeguarding government data. The objectives of this research are: (1) to measure the current maturity level of information security in Indonesian e-government institutions; (2) to develop a model based on international standards and local administrative context; and (3) to test the model's reliability and identify key influencing factors on security readiness. Using a quantitative approach, data were collected through surveys from 140 respondents across various government agencies. The model incorporates technical, managerial, and cultural domains, including governance, risk management, asset management, frameworks, technology and information security, organizational culture, and institutional characteristics. Model development drew on literature, national standards (e.g., BSSN's KAMI Index), expert input, and empirical testing. A structured questionnaire using Likert-scale items was developed and validated through pilot testing. Data analysis included descriptive statistics, confirmatory factor analysis, and Structural Equation Modeling (SEM) via Smart-PLS. The instrument showed strong validity and reliability based on Cronbach's Alpha, Composite Reliability, and AVE metrics. The results revealed that technology and asset management are the most influential factors in determining information security maturity, while governance and risk management had weaker direct effects. Notably, organizational culture acts as a significant mediator linking governance with institutional characteristics. This model offers a practical diagnostic tool for government agencies to benchmark their security posture and guide strategic improvements. It also addresses a research gap by introducing a validated, locally relevant model that aligns with international standards. Broader application of this model is recommended to enhance the quality, reliability, and security of public services, with further studies encouraged to test its applicability in other sectors.

Keywords: Information security, maturity, model, e-government, index, Indonesia

APPROVAL

This is to certify that this thesis conforms to acceptable standards of scholarly presentation and is fully adequate, in quality and scope, for the fulfilment of the requirements for the degree of Doctor of Philosophy.

The student has been supervised by: **Professor Ts Dr Aedah Abd Rahman & Professor Dr Syopiansyah Jaya Putra**

The thesis has been examined and endorsed by:

Ts Dr Wan Fatimah Wan Ahmad,
Asia e University
Examiner 1

Assoc Prof Dr Najwa Hayaati binti Mohd Alwi,
University Sains Islam Malaysia (USIM)
Examiner 2

This thesis was submitted to Asia e University and is accepted as fulfilment of the requirements for the Degree of Doctor of Philosophy.

……

Prof Dr Siow Heng Loke
Asia e University
Chairperson, Examination Committee
(13 June 2025)

DECLARATION

I hereby declare that the thesis submitted in fulfilment of the requirements for the Degree of Doctor of Philosophy is my own work and that all contributions from any other persons or sources are properly and duly cited. I further declare that the material has not been submitted either in whole or in part, for a degree at this or any other university. In making this declaration, I understand and acknowledge any breaches in this declaration constitute academic misconduct, which may result in my expulsion from the programme and/or exclusion from the award of the degree.

Name: Faiz Muqorrir Kaaffah

Signature of Student: **Date**: 13 June 2025

ACKNOWLEDGEMENTS

Praise and gratitude are due to Allah SWT for all His mercy and grace so that the author can complete this thesis well. On this occasion, the author would like to express his sincere gratitude to the Supervisor, Prof. Ts. Dr. Aedah Abd Rahman, and also to the Co-Supervisor, Prof. Dr. Syopiansyah JayaPutra for providing guidance, direction, and support that were very meaningful during the research process. All the advice and criticism provided have helped the author to improve and refine this work.

The author is also grateful to all the lecturers and staff in the ICT Doctoral Program for providing valuable knowledge and inspiration. The author also extends his deepest gratitude to his beloved family, especially to Ibu Ciawi, Galuh beloved wife, Sahila and Risyad, and the extended family in Ciawi and Bandung, who always provide unstinting moral and material support.

Not to forget, the author appreciates his fellow students who have been discussion partners, Mr Beki, Mr Manaf, and Mr Cepi, and fellow lecturers at UIN Bandung and UIN Siber Cirebon, who supported each other during this process. Finally, the author would like to thank all respondents who have taken the time to participate in this research. Hopefully, this thesis can provide benefits for readers and make a positive contribution to the development of knowledge in the field of Information Communication and Technology (ICT).

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

CA	Cronbach's Alpha
CND	Conditioning and Distribution
CR	Composite Reliability
ICT	Information Communication and Technology
IDS/IPS	Intrusion Detection and Prevention System
ISMS	Information Security Management System
IT	Information Technology
PDCA	Plan-Do-Check-Act
PLS	Partial Least Square
SSO	Single Sign-On

CHAPTER 1

INTRODUCTION

In an increasingly competitive era of globalization, the use of information and communication technology (ICT) has become one of the main pillars supporting the transformation of public services. In the environment of public service providers, the use of ICT continues to experience rapid growth along with the community's need for fast, reliable, and safe services. However, this development cannot be separated from the various challenges that accompany it, especially related to threats to information security.

Information security includes three main aspects: confidentiality, integrity, and availability. Disruption of any of these aspects can cause a decrease in service quality and have a negative impact on the performance of public service providers. As one of the important elements in good corporate governance, the role of information resources and ICT is becoming increasingly crucial in realizing quality public services (Farn et al., 2022).

Information security models have different characteristics in each country, which are caused by various factors, such as the political system, legal system, economic situation, available technological infrastructure, internet penetration, computer devices, availability of human resources, digital literacy levels, and ethnic diversity in terms of norms, language, and expertise (Wahyuni, 2020). This condition shows that the information security approach cannot be applied uniformly in all countries, including Indonesia.

In the context of e-government, information security initiatives in developed countries often begin with the design of a strategic, integrated system that spans across all relevant governmental institutions. This is typically followed by a systematic

evaluation to identify both strengths and vulnerabilities. Based on this assessment, a strategic security framework is formulated—one that addresses both technical and non-technical dimensions. Technical factors include infrastructure, cybersecurity technologies, and protocols, while non-technical factors encompass human resource capacity, governance structures, and institutional processes. Recent frameworks, such as those recommended by the OECD (2022), emphasize the importance of aligning these components to ensure cohesive digital security governance across government agencies (OECD, 2022).

Indonesia, as a developing country, continues to face significant challenges in implementing a mature and sustainable information security model within its e-government systems. Key obstacles include limited ICT infrastructure in rural and remote regions, a shortage of skilled cybersecurity professionals, and a digital literacy gap among the general population. According to a 2022 national digital transformation review by Bappenas and Kominfo, disparities in access, skills, and governance readiness persist across central and local agencies. Therefore, it is crucial to develop an information security maturity model that is contextually relevant to Indonesia's socio-technical landscape to ensure long-term sustainability and effectiveness of digital government initiatives (Kominfo & Bappenas, 2022; UNDESA, 2022).

This research aims to discuss the size of the maturity of the information security model in e-government systems in Indonesia. This research is based on the realities and problems previously identified, with a focus on developing reliable information security services that meet national needs. Hopefully, the results of this research can contribute to the development of a better information security strategy to support effective governance.

1.0 Background of The Study

In the era of globalization, the development of communication and computer technology has brought major changes in governance, including in Indonesia. The use of this technology enables the creation of better governance, known as good governance, which is characterized by transparency, accountability, community participation, and improved quality of public services. Technology helps the government speed up decision-making, reduce manual workload, and improve administrative efficiency. With a digital system, the government can also provide faster and more transparent public services to the community.

The utilization of information technology also provides opportunities for the public to participate more actively in government processes. Digital platforms such as online surveys, public consultations, and public complaint applications make it easier for citizens to convey their aspirations. In addition, technologies such as e-government, e-budgeting, and e-procurement have helped the government minimize the potential for corruption, collusion, and nepotism practices, thus creating cleaner and more trustworthy governance.

Indonesia is undergoing fundamental changes in national governance, characterized by efforts to strengthen democracy, transparency, digital transformation, and rule of law. These changes create opportunities to realign public administration with citizen-centered policies and more accountable governance structures (Kementerian PANRB, 2021).

However, Indonesia still faces major challenges in applying technology to support governance. One of the main challenges is the digital divide. Uneven access to technology, especially in remote and rural areas, hinders the government's efforts to provide inclusive digital services. In addition, the rigid culture of traditional

bureaucracy often slows down the adoption of technological innovations in various government sectors.

On the other hand, threats to data security are a serious issue in the implementation of digital technology. Hacking, data leaks, and cyberattacks can threaten public trust in government digital systems. In addition, the competence of human resources (HR) in the government sector is also a challenge that must be overcome. Many government employees have not fully mastered information technology, so training and developing HR competencies are important steps in ensuring the success of technology implementation.

Indonesia is currently in a transformation phase towards a democratic, transparent, and rule-of-law-based government. This change provides a great opportunity to reorganize the bureaucratic system and make the interests of the people the top priority. By utilizing communication and computer technology to the fullest, the government can improve public services, support national development, and create a more equitable environment that is oriented towards the interests of the wider community.

Presidential Instruction (Inpres) No. 3 Year 2003 on National Policy and Strategy for e-Government Development in Indonesia. The President has directed each Governor and Regent/Mayor to undertake the requisite actions in alignment with their respective responsibilities and authorities to facilitate the national implementation of e-government development.

The advancement of e-Government in Indonesia aims to establish a digital-based governance system to enhance the effectiveness, efficiency, and transparency of public service delivery. This transformation involves (1) digitalizing internal government procedures such as data processing, information management, and operational

workflows, and (2) leveraging digital innovations to make public services more accessible, affordable, and equitable across the country (Perpres 95/2018; KemenPANRB, 2021; UN DESA, 2022).

The transition to e-Government aims to establish and enhance electronic government through the extensive utilization of information and communication technology (ICT). Since the issuance of Presidential Instruction No.3 in 2003 on e-Government Development Policy and Strategy in Indonesia, government agencies should be able to utilize the potential of information and communication technology (ICT) to improve efficiency, effectiveness, transparency, and accountability. Despite the regulations, Indonesia is one of the countries where the implementation of e-Government is slow.

According to the United Nations E-Government Survey (UNDESA, 2022), e-Government is defined as the use of information and communication technologies (ICT), particularly the Internet, to deliver public services, engage citizens, and strengthen government institutions through both external and internal interactions. It emphasizes digital transformation to improve service quality, promote inclusive participation, and enhance transparency in governance (UNDESA, 2022).

In practice, the level of e-government readiness varies between countries (UNDESA, 2018; Elbahnasawi, 2014). Based on a survey from the United Nations (UN) in the 2018 EGDI (e-Government Development Index) publication, Indonesia is in 107th position in the world and 7th in ASEAN and is far below other ASEAN countries such as Singapore, Malaysia, Brunei Darussalam, Thailand, Philippines and Vietnam. Indonesia′s average EGDI value is also still below the Southeast Asian regional average with a value of 0.5555, while Indonesia only has a value of 0.5258 (UNDESA 2022). Then according to the UNDESA survey in 2022 related to the

implementation of the Electronic Based Government System (EBS), Indonesia was ranked 77th among 193 UN member countries. In addition, Gartner (2022) reported that more than 60% of e-Government initiatives fail, and the failure rate of e-Government projects in developing countries reaches 60-80%.

Currently, many e-Government systems in Indonesia, including those at the ministry and regional government levels, operate in isolation and lack interoperability. A 2023 analysis by Kompas noted over 27,000 separate government applications with limited integration, resulting in redundant platforms and user inconvenience.

To address this fragmentation, the Government enacted Presidential Regulation No. 95 of 2018 on SPBE, followed by Perpres No. 82 of 2023 to accelerate digital transformation and service integration. As of May 2024, the formation of GovTech Indonesia (INA DIGITAL) supports this strategy: BPS reported that 65 ministries and regional governments have successfully integrated their digital services into the national SPBE portal, demonstrating a significant step toward centralized data systems and unified service delivery (Kompas 2023; Sekretariat Kabinet 2024; BPS 2024).

The sophistication of e-Government implementation varies significantly across countries due to differing levels of ICT readiness, particularly in terms of infrastructure, digital skills, and interoperability. A framework analysis by Apleni & Smuts (2020) highlights that many developing countries face challenges like limited infrastructure, lack of interoperability, and insufficient human capacity. In the governance of ICT, information security plays a crucial role: the confidentiality, integrity, and availability (CIA triad) of information are foundational to maintaining system reliability and trustworthiness (Apleni & Smuts, 2020; ISO/IEC 27000:2018).

In general, the public expects government e-services to meet their information and service needs while ensuring security and privacy. Trust in e-government is

strongly linked to these guarantees. A study by Ulung Pribadi, Iqbal & Restiane (2021) in Indonesia demonstrated that privacy and security significantly influence public trust ($p < 0.001$), with an R^2 of 0.494. However, national surveys still report low trust levels in e-government platforms, largely due to inadequate data privacy and security provisions. Recent research by Fadrial et al. (2024) further highlights that perceived security and privacy are among the strongest predictors of trust in local e-government services. These findings underscore that effective privacy protection during citizens' interactions with e-government is essential for fostering public confidence. (Pribadi et al., 2021; Fadrial et al., 2024).

Low public trust in e-Government often stems from inadequate technical protection of information assets spanning preventive measures, secure data handling throughout collection, processing, storage, and input/output, and incident response which fails to safeguard confidentiality, integrity, and availability (CIA triad). A 2024 study by Fadrial et al. found that perceived security and privacy are the strongest predictors of public trust in Indonesian local e-Government services. In a comparative global assessment, Silva et al. (2023) revealed that many governments online service platforms remain vulnerable due to weak implementation of secure communication protocols, improper certificate management, and exposure to known vulnerabilities undermining user confidence worldwide (Fadrial et al., 2024).

Concerns over privacy breaches, malware, malicious code distribution, and fraud remain prominent, contributing to persistent public distrust in e-Government services. Rahman & Putri (2022) found that 38% of Indonesian citizens cite concerns over personal data leaks when using online government platforms. Moreover, Ginting et al. (2023) reported that 27% of users experienced exposure to phishing or malware threats in connection with e-Government applications, further eroding trust.

Table 1.1 presents the most common types of security and privacy incidents reported by users of e-Government services in Indonesia.

Table 1.1: Security Incident Types in E-Government in 2022

No.	Security Incident Types	Percentage
1	Virus	77.60%
2	Misuse of identity	34.40%
3	Account hijacking	19.20%
4	Financial fraud	5.90%
5	Break-in	2.00%

Sources: kominfo.go.id (2023)

Since 2017, BSSN (the National Cyber and Crypto Agency) has also identified the detrimental impact of cyber threats on electronic government systems. Apart from disrupting public services, cyberattacks can also damage the government's credibility. As a result, citizens become reluctant to utilize public services through online channels. Globally, a survey from Ovum ICT Enterprise Insights in 2016 cited cybersecurity as a major issue (20.1%) and a major challenge (53.1%). The issue of security from cyber threats is increasingly prominent because people are anxious about the government's ability to handle their personal data.

One of the major challenges faced by government agencies in Indonesia is the limited capacity to handle cybersecurity incidents. According to the 2022 BSSN security landscape report, GOV-CSIRT recorded 399 confirmed cyber incidents across government institutions, including data breaches and ransomware, affecting 285 stakeholders. Despite this increasing caseload, responses are still constrained at the national and regional levels. By September 2024, BSSN had established only 264 CSIRT teams (exceeding the RPJMN target of 131), highlighting uneven distribution and limited incident-handling coverage (BSSN GOV-CSIRT, 2023; GovInsider, 2024).

The presence of risks to information assets necessitates strong information security governance across all organizations, including government-operated public service agencies. This governance must include enhanced preparedness and vigilance against cyber threats, especially those targeting critical government infrastructure. According to the OECD (2022), a whole-of-government approach is essential to manage digital security risks and ensure the resilience of public services. Moreover, KPMG (2025) highlights that 65% of government organizations struggle with cybersecurity risk management due to limited understanding of emerging technologies and reliance on legacy systems. (OECD, 2022; KPMG, 2025).

The Indonesian government, through the Ministry of Communication and Information Technology (Kominfo), has issued repeated appeals to all public service providers and entities overseeing critical infrastructure to enhance their awareness and implementation of information security practices. For example, in February 2023, Kominfo collaborated with 12 universities to strengthen the digital safety pillar, highlighting the urgent need for increased cybersecurity awareness amid rising online fraud and phishing incidents. Furthermore, in September 2024, Kominfo's Digital Talent Scholarship initiative included a cybersecurity training program for over 2,450 government officials, reinforcing the commitment to foster a more robust cybersecurity culture across government institutions (Kominfo, 2023; Kominfo PROA, 2024).

To strengthen information security governance, the Indonesian government through the Ministry of Communication and Information Technology (Kominfo) has actively appealed to central and regional government agencies that provide public services. These efforts are carried out through a series of initiatives, including public awareness campaigns, technical guidance, and inter-agency coordination forums. In

addition to these efforts, the government has enacted multiple regulatory instruments, such as laws, ministerial regulations, circulars, and decrees, to institutionalize cybersecurity policies within government agencies. Notably, Ministerial Regulation No. 4 of 2016, Ministerial Circular No. 3 of 2021, and recent BSSN directives on SPBE security frameworks serve as foundational references for digital security practices in Indonesia's public sector (Kominfo, 2021; BSSN, 2023).

Therefore, based on the above background, the researcher here wants to discuss how the importance of information security based on the government's perspective and measure information security for e-government public services so that it can be new knowledge that can be applied to government services.

1.1 Problem Statement

The target of regulations, policies and efforts made by the government through the Ministry of Communication and Information Technology are to realize the implementation of information security governance within government agencies both at the central and regional levels. In implementing information security governance within government agencies, good readiness is needed, which includes several aspects, including infrastructure, planning, funds/financial, and human resource readiness. Thus, this study is intended to explore and evaluate the extent of the readiness of government agencies to implement information security governance (Wijatmoko, 2020).

The use of service and security standards to guide business processes can help organizations ensure robust IT security governance. However, many organizations struggle to understand the extent of implementation when multiple standards are applied concurrently. A 2023 ISACA Journal article highlights that deploying and complying with more than one standard frequently results in overlapping