Best practice framework for information technology security governance in Indonesian government

Rika Yuliana[1], Zainal Arifin Hasibuan[2]
[1]Information Technology Study Programme, State Islamic University Ar-Raniry, Banda Aceh, Indonesia
[2]Faculty of Computer Science, Universitas Dian Nuswantoro, Semarang, Indonesia

Article Info

Article history:

Received Aug 6, 2021
Revised Jun 12, 2022
Accepted Jul 7, 2022

Keywords:

Best practice
Digital government
Framework
Indonesia
Information and communication technology
Security governance

ABSTRACT

Information technology security is crucial for a digital government system to have so that the continuity of business processes can run smoothly. However, the current best practice of information security governance in the Indonesian national government is still inadequate according to various related studies still siloed and scattered and leading to vulnerabilities in the various digital services provided. Therefore, this study aims to develop a best practice framework for managing information security that is aligned with the needs of Indonesia's digital government. This research started by looking for the main framework of information security governance. Then the main components that resulted from that were benchmarked with other Information Security Governance (ISG) best practices from different countries. Finally, it ended up complementing them with information security parameters, other related components, and recommendations, particularly in the Indonesian context, so that the main components and their respective constituent sub-components can be obtained according to the needs of the Indonesian e-government. The cause-and-effect analysis concept analyses the data linkages between the six central components and their respective sub-components. This study concludes that each of main components and sub-components supports each other so that all these things must be carried out in a balanced and continuous manner.

Corresponding Author:

Rika Yuliana
Information Technology Study Programme, State Islamic University Ar-Raniry
Banda Aceh, Kopelma Darussalam, Aceh Province, Indonesia
Email: rika.yuliana@ar-raniry.ac.id

1. INTRODUCTION

Information security is a vital component in the planning process of integrated information technology in organizations, particularly in the Indonesian government [1]. This is caused by the fact that the government is in the process of developing digital government systems as well as smart cities altogether, so the security aspect is one of the major concerns for the government in providing a better service to stakeholders. Due to the need to maintain the quality of services provided by the Indonesian government in terms of confidentiality, integrity, and availability for digital government systems, the government should fulfill the needs of users up to the highest level of information technology security maturity. Furthermore, security aspects are linked to smart cities where cyber physical systems are not only used by citizens but can also be modified by hackers and identity thieves [2]. Based on several studies from references [3], [4] and facts from the real world [5], Indonesia, however, does not yet have a comprehensive best-practice framework for managing information security. It affects many services that have not been utilized optimally due to the vulnerability of malware attacks, crashes, and other related problems.

Various issues and problems that arise from the use of e-government technology in Indonesia increase day by day, especially those related to information security. For example, the vulnerability of a government website being hacked by irresponsible parties can result in disruption of the services that can be provided to the community. It can also create a bad stigma in the community. Although the government and related stakeholders are concerned with the importance of information security in e-government services, which can be seen in the integration of security aspects in the implementation of Indonesia’s digital government and various related research, there are still gaps in the application of information security governance. It can happen because the researchers involved have only looked at information security in Indonesia from a technical standpoint. Thus, it also causes various impacts on the lives of Indonesian society members, such as identity theft. Moreover, the study shows that this challenge needs to be addressed in three ways: the development of governance's practicality, adaptability, and measurability, and its subsequent alignment with the organization [6]. Therefore, Indonesia's government should have comprehensive guidance on how to govern information security, particularly in the form of best practices derived from related frameworks and governance for reaching the highest level of information security maturity in the implementation of Indonesia’s digital government as the country is still evolving and growing.

According to [7], security has evolved from a narrow and specific isolated issue to a strategic business problem with "from the basement to boardroom" implications. The main point is that organizations must protect themselves. Moreover, they must also develop strategies to ensure that their businesses are resilient enough to exploit the opportunities relating to the digitalization. Besides that, information technology governance is a component of organizational governance that entails the role and implementation of relational processes, structures, and mechanisms. It allows business and information technology (IT) stakeholders to do the tasks of promoting business or IT alignment and the formation and protection of IT business value. The "Infrastructure State" evaluation assesses the extent to which IT has been able to sustain the robust and reliable infrastructure required to meet business needs effectively. It is accomplished by comparing each platform domain to risk-based criteria to assess the potential effect on business continuity, security, and/or compliance [8]. These problems, if not handled properly, will cause financial losses that will harm the business and jeopardize the sustainability of the organization both in the short and long term [9].

Information security must be flexible to handle every situation and a variety of requirements from different information, systems, or organizations [10]. Information security management (ISM) is a sustainable, structured and systematic approach within security for managing and protecting organizational information from being infiltrated by irresponsible parties. To ensure information remains secure, many organizations have implemented ISM by establishing and reviewing information security (IS) policies, processes, procedures and organizational structures. Organizations also need to validate some of the ISM factors and elements that contribute to the success of ISM to guide practitioners in implementing proper ISM [11].

There are numerous standards, frameworks, laws, guidelines, and best practice references available to advise information security managers on how they implement security controls. A significant portion of these guidelines is only applicable to specific countries, particularly where the data protection and privacy rules are mostly implemented. These guidelines are also reinforced by the whole industry-specific advisors that can help the information security managers to inform executive managers about the best controls implementation to maintain businesses safety and security. The manager must also consider what is truly important for the organization and designs a security management system that is still relevant, proportionate, and takes it into account the organization's risk tolerance and the best approach to business continuity [12].

Today, in every organization, IT services must be provided in such a way that cost-effective, reduces security threats and complies with legal and regulatory requirements. The equations are challenging to solve and, in some cases, may seem impossible. In order to survive in this environment, the proposed information system security governance (ISS-GOV) model in the form of an internal repository seems appropriate for this purpose. Implementers currently have a framework for implementing IT strategies, plans and processes, for defining metrics, benchmarks, and auditing, as well as integrating security issues to reduce risk [13].

Based on these concepts and developments in the realm of information security, Indonesia urgently requires a comprehensive information security governance framework in accordance with the current development requirements of e-government systems. Basically, there is a relationship between aspects of information security and information technology governance as shown in Figure 1 and also a relationship between IT security and cyber security as shown in Figure 2 [14]. However, the study by [15] proves that cybersecurity governance in Indonesia’s government agencies is still lacking and not yet integrated and the need to combine various related matters [16]. Besides that, research shows that the continuous development of the Internet and technology, such as big data, means that public service information is getting more attention [17], while the maturity level of information security (cybersecurity) in Indonesia is still deficient [18], so that a proposed framework is required to manage information security in accordance with the needs of Indonesia's digital government to reach the optimum level of information security maturity. Therefore, this study aims to propose a best practice framework in information security governance so that it can be implemented in Indonesian e-government.

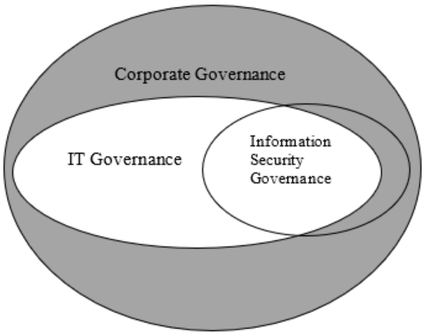


Figure 1. Information security governance positioned [14]

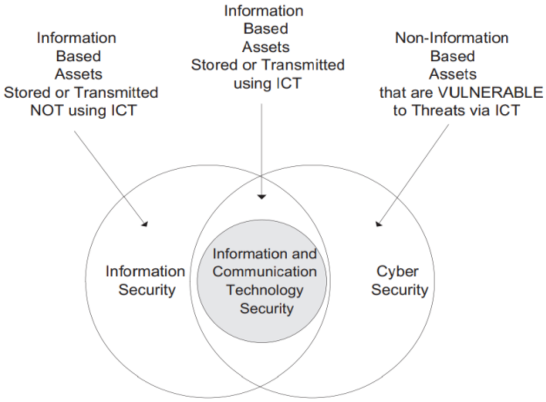

Information Based Assets Stored or Transmitted NOT using ICT
Information Based Assets Stored or Transmitted using ICT
Non-Information Based Assets that are VULNERABLE to Threats via ICT
Information Security
Information and Communication Technology Security
Cyber Security

Figure 2. The relationship between information and communication security, information security and cyber security [14]

2. RESEARCH METHOD

Basically, information security is a crucial matter that works integrated with organizational governance and is related to data management, applications, business processes and infrastructure/technology [19] so that it affects various organizational management activities from the operational level to the strategic level of the organization [14]. In addition, there are multiple stages involved in the security life cycle process in the information security development process. It starts from the set of assessing, designing, implementing, and maintaining information assets under security principles [20]. Therefore, the components of the information security best practice framework for digital governance in Indonesia are arranged in line with these concepts, which are adjusted to several standards, frameworks, laws, guidelines, and best practice references related to the Indonesian national context.

In carrying out activities to develop a framework for best practice in information security for the Indonesian electronic government system, this involved various prior studies resulting from the incorporation of related frameworks and recommendations from experts who are proficient in information security. When the concepts of both frameworks are applied in parallel, they create synergy that benefits all high-level areas of an organization. By combining these principles, a comprehensive set of rules that embraces and secures the business while also cultivating an IS culture can be created for information security governance (ISG) implementation. Nevertheless, it has the potential for misinterpretation, so organizations should act in one direction first, e.g., business-oriented, then in another, e.g., security-oriented, and finally to synthesize [21]. Based on that fact, this study was begun by looking for the main framework of information security governance that comes from a combination of the cyber-physical system (CPS) security governance model [22] and several critical success factor (CSF) components of information security derived from [23] and [24] based on the concept developed by [25]. Then the main components were benchmarked [26] with other ISG best practices stemming from other related countries to get practical insights and lessons learned to refine these critical components. In the final stage, these main information security governance components were complemented by information security parameters [27], other related components [28], and recommendations [29], particularly in the Indonesian context, so that the main components and their respective constituent subcomponents were able to be merged altogether, resulting in relevant activities according to the needs of Indonesian e-government. The research method can be illustrated in Figure 3, followed by detailed research steps in conducting the first step of the research methodology as shown in Figure 4.

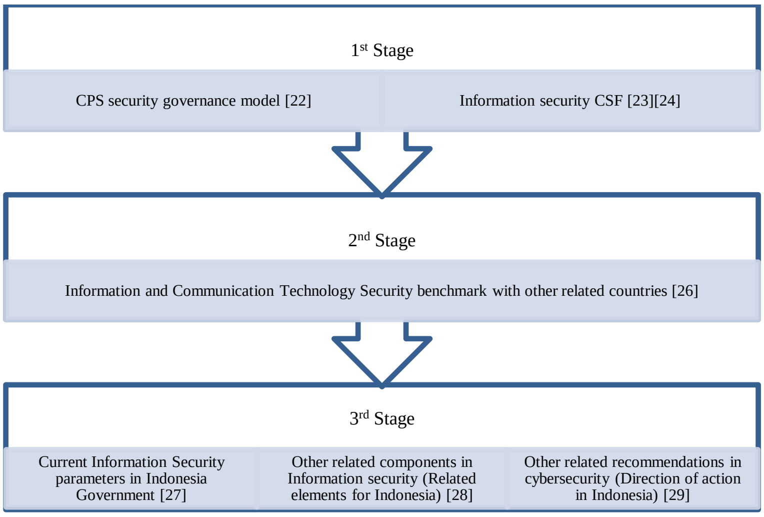
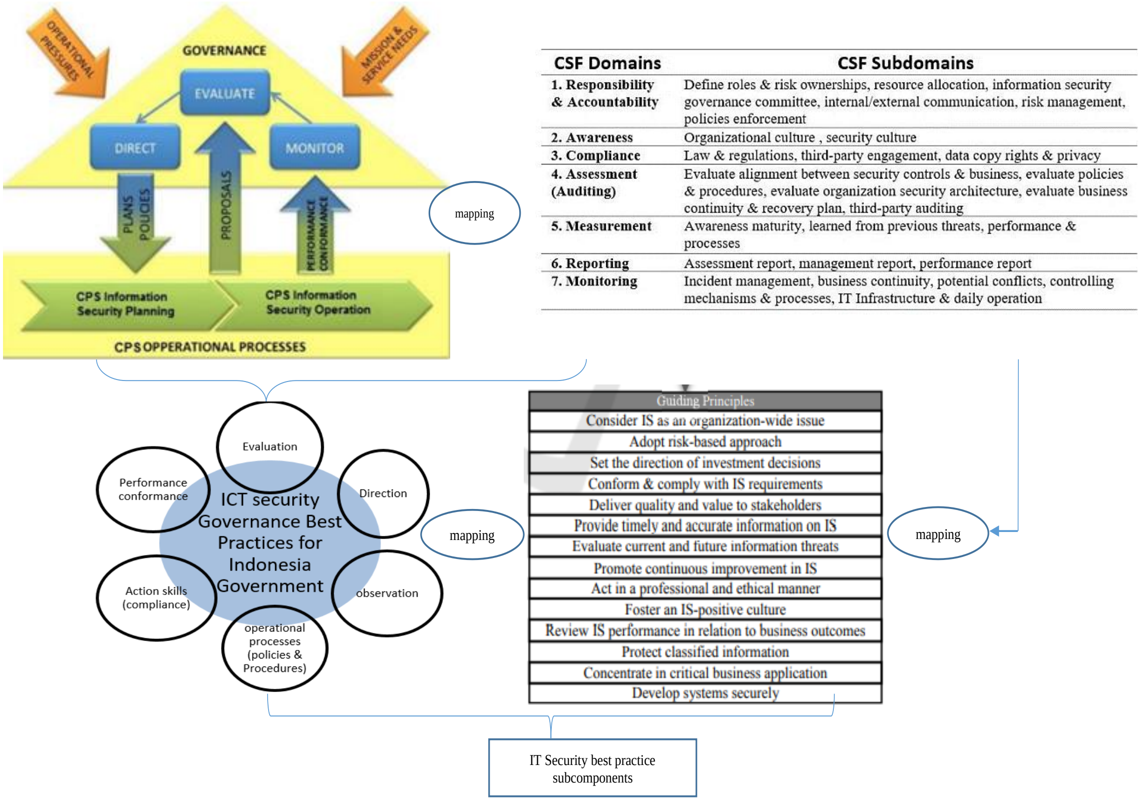

1st Stage
CPS security governance model [22]
Information security CSF [23][24]
2nd Stage
Information and Communication Technology Security benchmark with other related countries [26]
3rd Stage
Current Information Security parameters in Indonesia Government [27]
Other related components in Information security (Related elements for Indonesia) [28]
Other related recommendations in cybersecurity (Direction of action in Indonesia) [29]

Figure 3. Research methodology


OPERATIONAL PRESSURES
GOVERNANCE
MISSION & SERVICE NEEDS
EVALUATE
DIRECT
MONITOR
PLANS POLICIES
PROPOSALS
PERFORMANCE CONFORMANCE
CPS Information Security Planning
CPS Information Security Operation
CPS OPPERATIONAL PROCESSES
mapping
Evaluation
Performance conformance
Direction
ICT security Governance Best Practices for Indonesia Government
Action skills (compliance)
observation
operational processes (policies & Procedures)
mapping
mapping
IT Security best practice subcomponents

CSF Domains	CSF Subdomains
1. Responsibility & Accountability	Define roles & risk ownerships, resource allocation, information security governance committee, internal/external communication, risk management, policies enforcement
2. Awareness	Organizational culture , security culture
3. Compliance	Law & regulations, third-party engagement, data copy rights & privacy
4. Assessment (Auditing)	Evaluate alignment between security controls & business, evaluate policies & procedures, evaluate organization security architecture, evaluate business continuity & recovery plan, third-party auditing
5. Measurement	Awareness maturity, learned from previous threats, performance & processes
6. Reporting	Assessment report, management report, performance report
7. Monitoring	Incident management, business continuity, potential conflicts, controlling mechanisms & processes, IT Infrastructure & daily operation

Guiding Principles
Consider IS as an organization-wide issue
Adopt risk-based approach
Set the direction of investment decisions
Conform & comply with IS requirements
Deliver quality and value to stakeholders
Provide timely and accurate information on IS
Evaluate current and future information threats
Promote continuous improvement in IS
Act in a professional and ethical manner
Foster an IS-positive culture
Review IS performance in relation to business outcomes
Protect classified information
Concentrate in critical business application
Develop systems securely

Figure 4. Detailed research steps in the first stage of research methodology

3. RESULTS AND DISCUSSION

Research conducted by [7] revealed that security should be seen as an indispensable feature in a digital context. Therefore, organizations need to start adjusting digital security governance according to their current needs. The study supports practitioners and decision-makers on how organizations and their security approaches are impacted by digitalization. Thus, in this section, the results from each stage are discussed within each sub section in order to get clear explanations about the results.

3.1. Key components from stage 1

Based on the stages listed in the research method, the results of a proposed best practice framework for information security in the Indonesian government are obtained, consisting of six main frameworks and then the sub-components of each of these main frameworks, namely evaluation, direction, observation, performance conformance, action skills (compliance), and operational processes (policies and procedures). The six main best practice frameworks for information technology security for the Indonesian government can be seen in Figure 5. These six things are interrelated to one another so that if one component or sub-component is ignored, it will affect overall performance. It will have the potential to weaken the ongoing governance system. Therefore, it is necessary to have synergistic coordination between the two at a strategic level so that the balance and compatibility between them can be adequately maintained so that the objectives of the Indonesian government can be achieved. Each component and subcomponent needs to be assessed for the effectiveness of each to suit the system requirements.

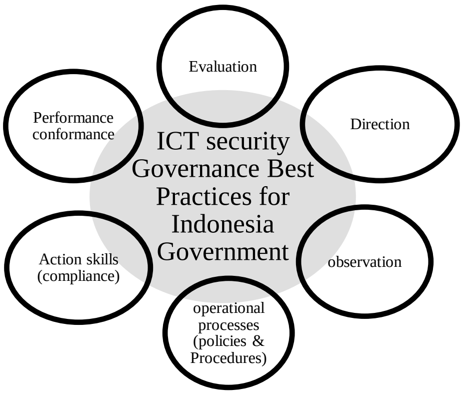

Evaluation
Direction
observation
operational processes (policies & Procedures)
Action skills (compliance)
Performance conformance
ICT security Governance Best Practices for Indonesia Government

Figure 5. Key components of information technology security best practice framework for Indonesian government

3.2. Results from stage 2 (benchmarking the results from the first stage with existing Information and Communication Technology (ICT) governance best practices in certain countries)

Current practices of ICT governance in several countries are facing rapid changes due to various challenges coming to government territory. Therefore, they need to establish a secure system for digital government in order to be ready and take proper action when dealing with security issues. In the following paragraphs, a brief discussion of information and communication technology security governance best practices from related countries is presented by taking into account key aspects in Indonesia digital government [30], [31], which consists of United States, Malaysia and Africa because of the political system, human resources index and geolocation closed similarities with Indonesia respectively.

The American government has a unique way of governing physical and cyber security functions applied across many issues and many interdependent stakeholders. The steps have been developed and implemented in such a way over many years. They continue to be improved and are the outcome of progressing commitment by different pioneers from the state official and administrative branches of government, education, private and not-for-profit organizations. Over the five states, governors have come up with leadership and responsibility for this issue [32]. The functional aspects included in the security framework consist of identify, protect, detect, respond, and recover and each of these aspects is accompanied by their respective components and subcomponents [33].

Data collected by [34] through document analysis and interviews has confirmed that the ISG is present in several Malaysian public sector documents. The element in the ISG came from a combination of the information security aspects of ICT with non-ICT so that an ISG policy has become complete and does not overlap. The development of the ISG framework has been an integrated program involving policy-making institutions in public sector administration in Malaysia. Integrated development has resulted in a comprehensive ISG framework for use by public sector agencies in Malaysia. The components are governance approaches, good practices, risk management, organizational management, training and awareness, implementation methods, and laws and regulations. The four components will undergo a continuous cycle of design, implementation, assessment, and follow-up processes. These elements could be combined with Malaysia's cybersecurity principles [35].

The information security model that applies in Nigeria has been emphasized in the general aspect of security. The model shows how e-government systems relate to their customers by using two-way certificate authentication with valid user authentication for each service. After the authentication point, users log in and run the specified service. This system ensures that all communications between parties within the e-government infrastructure are encrypted. The framework recommended the use of session keys because session keys are randomly generated, making it difficult for attackers to intercept messages on the network. This framework has security middleware, which is basically the link between the public key infrastructure system and the application. All applications run to ensure that the system is generally safe. This middleware acts as an interface between applications, access controls, server management, cryptographic tools, and other important physical mechanisms. Role-based access control allows for proper assignment of responsibilities based on the policies specified in the strategic framework and is primarily based on hierarchical considerations. This allows system administrators to dynamically manage user access, making it easier to see who, where, when, and when the connection was initiated. Valid users who gain access are also identified and reported accordingly [36].

These main components of information technology security governance (ITSG) for Indonesia's e-government resulting from the first stage are then compared with other countries in handling the same issues to refine them. By seeing Table 1, America has all of the main components, while Malaysia and South Africa have some of them. Nevertheless, these countries complement one another and can validate the research findings that Indonesia's digital government needs all of these components to adequately protect the digital system in running the daily operations with its related stakeholders.

Table 1. Comparing main components of ITSG

Key Components	Country			
	USA	Malaysia	South Africa	Indonesia (Results)
Evaluation	√			required
Direction	√	√		required
Observation	√	√	√	required
Operational processes (policies and procedures)	√	√		required
Action skills (compliance)	√	√	√	required
Performance conformance	√		√	required

3.3. Results from stage 3

In this section, each of the key components which have been benchmarked with certain related countries is discussed one by one in more detail. When discussing each key component, they are elaborated with current information security parameters, related elements, as well as recommendations in the Indonesia context, specifically in order to acquire a complete/big picture of best practice framework in information security governance in the Indonesian government. However, it is also possible to see the gap within each best practice subcomponent as another outcome that cannot be avoided. Nevertheless, these gaps can be used for future developments in information security governance in Indonesia and other relevant nationalities.

3.3.1. Evaluation

The evaluation stage, often called the assessment stage or audit stage, serves an evaluation by using the CPS for current and future condition. Each electronic system administrator must examine and make judgments about current and future use of CPS by including strategy, filling, and provisioning arrangements (internal, external, or both). The reference of standard assessment follows common criteria (CC). It is a collection of globally and locally known as technical standards and configurations that enables the assessment of product safety and information technologies [22]. How people can assess information security for public administration requires a systematic approach that increases based on the needs of continuous improvement [37]. The evaluation model developed by Zuo [38] can be used as a benchmark accompanied by a socio-technical multidimensional approach [39]. The audit implementation relies on advanced standards and frameworks of IT infrastructure organization, management, and security such as Cobit and ISO 17799 [40].

Based on Indonesia government regulation no. 59 in 2020 concerning information security in particular evaluation which is claimed very important to support the management of Indonesia's e-government system, evaluation should be aligned with security goal. Moreover, an evaluation can be carried out by external parties through a maturity level assessment so that they can immediately start to optimize an information security system. Until now, the framework COBIT 5 [1] and ISO 27001: 2013 [41] are generally used to analyze the maturity level of information security systems especially in the Indonesia context [42]. Nevertheless, another way that can be used to assess the efficiency of information security is expert systems [43]. Therefore, Indonesia needs to combine these systems with other tools so that the following five sub-components are measured correctly and based on their needs. These five sub-components focus on evaluating alignment between security controls and business, evaluating policies and procedures, evaluating organization security, evaluating business continuity and recovery plan, and auditing the third-party.

3.3.2. Direction

The directing stage directly serves the preparation and implementation of various plans and policies to ensure that the use of CPS can connect with the objectives of the security system [22]. Besides, it can also be accomplished by highlighting and organizing the important points of information security policy, including the major challenges in the implementation with the need to review and enact policy in a perpetual process and thorough risk management framework [44]. This stage is necessary to find out the needs that must be improved from the existing information security system so that the system runs even better in the future.

3.3.3. Observation

In the observation/monitoring stage, there are two main functions of technology information in the security system, that are monitoring the conformity between the system and policies and monitoring the implementation of the system against the plan [22]. Moreover, the ongoing observation is considered to be an important factor enabling the potential risks, vulnerabilities, and threats that almost any institution may encounter on a regular basis [23]. A research study analyzes the theory of privacy, trust, commitment, and compliance to formulate a model that explains observed phenomena in real work environments. The research is done through monitoring organizational information in practice and makes a conclusion that monitoring information can improve the information security management (ISM) practices in organizations [45]. If the ISM practice works well, it will improve the overall organizational practice. There are 5 (five) important subcomponents in this observation component which can be seen in Table 2. Moreover, the recommended methods of monitoring information security [46], [47] can be utilized as guidance in implementing information security monitoring in Indonesia.

Based on the research results that are shown in Table 2, we can see that each of the best practice sub components needs further development because of the incomplete concrete activities that are available at this time. In the case of some best practice subcomponents such as incident management, business continuity, potential conflict and controlling mechanisms and processes, the availability of these activities in Indonesia's government is still missing, even though related research and recommendations have emerged. Moreover, in terms of IT infrastructure and daily operation subcomponent, Indonesia has given attention to this part from a technology point of view, but the relevant activities are miserable. Thus, for all activities within these best practice subcomponents, needs to be developed by merging the related parameters, elements, and recommendations. For instance, we can develop various activities based on related elements available within incident management, such as how to handle physical and logical threats. Other than that, in controlling mechanisms and processes subcomponents, the related elements need to be developed in such a way to establish a unit to monitor and control the national IT infrastructure.

3.3.4. Performance conformance

The performance and change of the organization are both ongoing, and both are required to track and evaluate whether the ISG principles, policies, and procedures are operating in accordance with the predetermined indicators and criteria [23]. Measuring information security performance is a vital component of the information security in the management system of the organization. According to a study, information security is purposefully defined and applied, but the measurements are principally implemented in the technical and operational levels, while strategic management remains inadequate [39]. Therefore, the three best practice subcomponents in the performance conformance domain that can be seen in Table 3 are important goals to achieve. The implementation of the performance conformance activity involves measuring and reporting the information so that performance can be compared in each period of time.

For the sake of performance conformance, the Indonesian government still has no idea what kind of activities to handle each of these best practice subcomponents, particularly in terms of providing timely and accurate information on IS performance, reviewing IS performance in relation to business outcomes, and promoting continuous improvement in IS. As a result, even if certain related elements or recommendations are unavailable for some parts, we must develop these activities based on those two. For instance, in terms of providing timely and accurate information on IS performance, we should combine these terms between reporting elements and recommendations in the reporting system in order to develop various activities relating to this subcomponent part. This is certainly done without ignoring the elements related to information security in Indonesia.

Table 2. Subcomponent of observation activities

Best practice subcomponent	IS parameters in Indonesia Government [27]	Related elements for Indonesia [28]	Direction of action in Indonesia (recommendations) [29]	Results/to be (ITSG activities)
Incident management	-	threat/attack: physical threat/attack, logical threat/attack	-	Need further development
Business continuity	-	management procedure: asset, incident, business continuity, operational, risk management	-	Need further development
Potential conflict	-	environment: politic, social, economy.	-	Need further development
Controlling mechanisms and processes	-	-	Establish a unit under the related government ministry to formally monitor and control national infrastructure to help ensure Indonesia's security and resilience.	Need further development
IT infrastructure and daily operation	Technology	Technology	-	Need further development

Table 3. Subcomponent of performance conformance activities

Best practice subcomponent	IS parameters in Indonesia Government [27]	Related elements for Indonesia [28]	Direction of action in Indonesia (Recommendations) [29]	Results/to be (ITSG activities)
Provide timely and accurate information on IS performance	-	Measuring: awareness maturity, learned from previous threats, performance and processes.	-	Need further development
	-	Reporting: assessment report, measurement report, performance report.	Create a single reporting system for electronic system operators for public services to report and disclose cybercrime incidents and data breaches, so that action can be taken.	Need further development
Review IS performance in relation to business outcomes	-	-	Review existing legislation to ensure that it remains relevant and effective in fighting cybercrime.	Need further development
Promote continuous improvement in IS	-	-	Strengthen law enforcement & prosecutors' capabilities to investigate cybercrime and bring those responsible to justice.	Need further development

3.3.5. Action skills/compliance

Compliance with laws and regulations is critical and becomes one of the key elements to ensure the ISG of the organization is effective and sustainable [23]. External rules and regulations frequently govern an organization's ability to collect information, conduct investigations, and control the networks among other activities of the information gotten from technology security. Besides, the organization should develop some requirements to comply with these rules to protect and design new systems and applications, and also determine how long to store data, or to do encrypting and tokenizing the sensitive data [48].

Two main types of compliance are regulatory compliance and industry compliance. Non-compliance has various consequences depending on the set of rules in question. In the case of industrial compliance, loss of privileges related to compliance can occur. In the case of regulatory compliance, non-compliance can effect harsher penalties, including detention for violating the relevant law [48].

According to a study, coercive pressure, normative pressure, and mimetic pressure have a significant influence to the organizational information of security compliance. It implies that the advantages of information security compliance encourage the management to enhance their commitment for information security compliance [49]. However, the level of awareness in terms of compliance with information security also needs an attention [50].

Based on these concepts, the important subcomponents relating to compliance can be seen in Table 4. There is only one best practice subcomponent in the context of compliance, namely conforming to and complying with internal and external information security requirements. The subcomponents consist of law and regulations, third party engagement, data copy rights, and privacy. As shown from Table 4, Indonesia still has not yet given any attention to the three of the constituent elements of this subcomponent because of the absence of information security parameters. In this context, Indonesia's government needs to develop the respected activities within this subcomponent by merging the related parameters, elements, and recommendations. For example, in third party engagement, the elements of cooperation and recommendation in creating and building dedicated civilian and military capabilities need to be merged and expanded so that they can create various activities within this context in accordance with Indonesia's government requirements.

Table 4. Subcomponent of compliance activities

Best practice subcomponent		IS parameters in Indonesia Government [27]	Related elements for Indonesia [28]	Direction of action in Indonesia (Recommendations) [29]	Results / to be (ITSG activities)
Conform and comply with internal and external IS requirements	law and regulations	-	Laws and regulations	Develop a standard marketing strategy to promote privacy online for protecting personal data.	Need further development
	Third party engagement	-	Cooperation: Governmental, National, and International.	Create and build dedicated civilian and military capability to help ensure that Indonesia has the capability to protect national interests in cyberspace.	Need further development
	Data copy rights and privacy	-	Legal: computer fraud, illegal access, data interference, copyright violation, child pornography.	-	Need further development

3.3.6. Operational processes (policies and procedures)

Determining the policies or procedures may be relevant to protect specific types of information (e.g. source code for complex software products). In this case, organizations must consider how valuable the information is, what the existence of the harm get experiences, and whether the decreasing risk is worth the cost (money or inconvenience) of protective measurement such as restricted access and others [51]. Most organizations recognize the needs of monitoring and improving the management of risk and internal security processes by using security governance procedures [52]. In addition, it also needs to be supported by policies that can be developed [53] and reused [54] to adapt with the changes of the organization. There are 10 (ten) important subcomponents in the operational activities of making policies and procedures in the information technology security as can be seen in Table 5.

In this context, for some parts, it is easier to create various activities relating to each best practice subcomponent because of the presence of a set of information security parameters, elements, and recommendations such as protecting classified information. Due to the fact that the related IS parameters in the Indonesian government are not comphrehensive yet, the relevant activities cannot be generated. Nevertheless, in other parts, it is taking more effort to create the activities because of the absence of either related parameters, elements, or recommendations such as an effective business continuity or disaster recovery plan. As a result, further development for various activities in each subcomponent is important in order to govern information security in Indonesia's digital government system holistically.

Overall, this study provides general results in regard with the six main components and each of the supporting sub-components. Moreover, by using the concept of cause-and-effect analysis [55] in analyzing the data linkages between the six main components along with their respective sub-components, it is concluded that there are strong relationships between one component and another components. If one component is neglected or not implemented properly, it will result the disruption of the overall information security system. It can be seen from the process of components (both in the form of policies and procedures) that are running. Nevertheless, if these components are not regularly reviewed, the level of effectiveness in achieving government performance will be difficult to be measured. It makes a result of difficulties when finding solutions to various complaints from users.

Table 5. Subcomponent of operational processes activities

Best practice subcomponent	IS parameters in Indonesia Government [27]	Related elements for Indonesia [28]	Direction of action in Indonesia (Recommendations) [29]	Results/to be (ITSG activities)
Consider IS as an organization wide issue:				
a. integrate IS with business activities	Work program and strategy	-	Develop a national cybersecurity strategy (NCSS).	Need further development
b. on-going strategic alignment	-	-	Promote cybersecurity requirements in government procurement processes for managing the national cyber defense.	Need further development
c. determine clear IS roles and responsibilities and be held accountable.	-	Security services: Prevent, Detect, Response. Security goals: confidentiality, integrity, availability, privacy, authenticity, non-repudiation.	Promote greater levels of trust in online services, such as e-government and e-commerce services.	Need further development
Act in professional and ethical manner	“IS Governance”	Organization: Committee (policy and coord.), operations centre, emergency response team.	Strengthen the role and coordination function of ID-SIRTII/CC as a national CERT.	Need further development
Deliver quality and value to stakeholders:				
a. Effective communication	-	-	Develop a cybersecurity communication strategy to strengthen and expand the national cybersecurity campaign.	Need further development
b. Effective business continuity/disaster recovery plan	-	-	-	Need further development
Adopt risk-based approach	“IS Risk Governance”	-	-	Need further development
Protect classified information	“Asset Governance”	Assets: Tangible, Intangible.	Create a formal list of CNIs on multi-stakeholder consultation, and work with the companies that own and manage CNIs.	Need further development
Concentrate on critical business applications	-	-	Establish emergency response asset priorities in the event a service failure occurs that are aimed at reducing impact.	Need further development
Develop systems securely	ISG Framework	-	-	Need further development
Foster an IS positive culture (organizational and security culture [56])	-	Security culture: Collective Values, Norms and Knowledge, Basic Assumptions and Beliefs, Artefacts and Creations.	Develop a single authoritative online portal for cyber raising awareness amongst governments, businesses, and civil society across the country. Raise awareness amongst senior government officials and board members of the critical national infrastructure operators of the cyber risks, and actions they can take to protect security-sensitive information.	Need further development
	-	Human competency: Sec. operation and management, ethical hacking, computer forensics, Sec. programming, Sec. implementation and Conf., Sec. architecture and Dev., Sec. Policies and Dev, cryptography, Sec. analysis	Provide incentive-based cybersecurity solutions for local cybersecurity products or the cyber insurance marketplace. Conduct crisis management exercises at a national level by inviting the relevant key national stakeholders to ensure preparations for national cyber incident responses are well managed and robust. Promote cybersecurity training and education programs designed for all employees at all levels in government organizations, state-owned enterprises, private critical infrastructure providers, and small-medium enterprises.	Need further development
Set the direction of investment decisions	-	-	Identify a center of excellence in cybersecurity research and education to locate strengths and providing focused investment to address gaps. Create a national-level register for information assurance and cyber security experts across the public and private sectors as a way of bringing new talent into the profession.	Need further development

Based on the research results obtained from all three stages, it can be seen that several activities generated have not been optimal within each subcomponent in terms of existing IS parameters for the Indonesian government, related elements, and sets of recommendations. Therefore, all the activities inside each subcomponent should be merged and developed according to the needs already described in each component to fulfill a broader picture of IT security governance requirements. Moreover, this is due to the lack of synergy between the current implementation of IT governance and IT security governance, so the activities related to information security governance need to be improved for their effectiveness in the Indonesian digital government context and future needs. In addition, information technology security in Indonesia needs to be continuously developed in line with the development of information technology infrastructure and the lifestyle fulfillment of society in the future.

4. CONCLUSION

This study concludes that there are six main components to compiling the best practice framework for information security governance that can be used by the Indonesian government, which consists of evaluating, directing, monitoring, performance conformance, action skills (compliance), and operational processes (policies and procedures) components. Each of the main components and sub-components supports each other, so all these things must be carried out synergistically and proportionately. Within each of these main components and the supporting sub-components, relevant activities can be generated but still need further development. Knowing that there are still inadequate activities within each of the subcomponents, it is necessary to develop them continuously for future needs. Their effectiveness also needs to be analyzed following the needs of the Indonesian national government in the future. Nevertheless, this best practice framework for information security governance must be aligned with information technology governance, which has implications for the IT architecture in the organization.

REFERENCES

[1] R. Umar, I. Riadi, and E. Handoyo, “Information system security analysis based on COBIT 5 framework using capability maturity model integration (CMMI),” (in Bahasa), *Jurnal Sistem Informasi Bisnis*, vol. 9, no. 1, pp. 47–54, May 2019, doi: 10.21456/vol9iss1pp47-54.

[2] F. Khan, R. L. Kumar, S. Kadry, Y. Nam, and M. N. Meqdad, “Cyber physical systems: a smart city perspective,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 4, pp. 3609–3616, Aug. 2021, doi: 10.11591/ijece.v11i4.pp3609-3616.

[3] M. Rizal and Y. Yani, “Cybersecurity policy and its implementation in Indonesia,” *JAS (Journal of ASEAN Studies)*, vol. 4, no. 1, Aug. 2016, doi: 10.21512/jas.v4i1.967.

[4] K. Kautsarina, O. Rafizan, A. B. Setiawan, and A. S. Sastrosubroto, “Information and communication technology service industry development in Indonesia,” *Australian Journal of Telecommunications and the Digital Economy*, vol. 5, no. 3, pp. 50–82, Sep. 2017, doi: 10.18080/ajtde.v5n3.96.

[5] D. Kardono, “Material 5: SPBE safety,” (in Bahasa), Ministry of Administrative Reform and Bureaucratic Reform, 2020.

[6] W. W. Lidster and S. S. M. Rahman, “Obstacles to implementation of information security governance,” in *17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, Aug. 2018, pp. 1826–1831, doi: 10.1109/TrustCom/BigDataSE.2018.00276.

[7] S. Leonelli, “Data governance is key to interpretation: reconceptualizing data in data science,” *Harvard Data Science Review*, vol. 1, no. 1, Jun. 2019, doi: 10.1162/99608f92.17405bb6.

[8] S. De Haes and W. Van Grembergen, *Enterprise governance of information technology: achieving strategic alignment and value in digital organization*. Boston, MA: Springer US, 2009, doi: 10.1007/978-0-387-84882-2.

[9] N. Shariffuddin and A. Mohamed, “IT security and IT governance alignment,” in *Proceedings of the 3rd International Conference on Networking, Information Systems and Security*, Mar. 2020, pp. 1–8, doi: 10.1145/3386723.3387843.

[10] B. Lundgren and N. Möller, “Defining information security,” *Science and Engineering Ethics*, vol. 25, no. 2, pp. 419–441, Apr. 2019, doi: 10.1007/s11948-017-9992-1.

[11] M. Zammani and R. Razali, “An empirical study of information security management success factors,” *International Journal on Advanced Science, Engineering and Information Technology*, vol. 6, no. 6, pp. 904–913, Dec. 2016, doi: 10.18517/ijaseit.6.6.1371.

[12] T. Campbell, *Practical information security management : a complete guide to planning and implementation*. Apress Publisher, 2016.

[13] M. Zaydi, “A conceptual hybrid approach for information security governance,” *International Journal of Mathematics and Computer Science*, vol. 16, no. 1, pp. 47–66, 2021.

[14] S. H. von Solms and R. von Solms, *Information security governance*. Boston, MA: Springer Science and Business Media, 2009, doi: 10.1007/978-0-387-79984-1_1.

[15] H. Ardiyanti, “Cyber-security and its development challenges in Indonesia,” (in Bahasa), *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, vol. 5, no. 1, pp. 95–119, 2014.

[16] Z. Mounia and N. Bouchaib, “A new comprehensive solution to handle information security governance in organizations,” in *Proceedings of the 2nd International Conference on Networking, Information Systems and Security*, 2019, pp. 1–5, doi: 10.1145/3320326.3320382.

[17] C. Wang and X. Jin, “The researches on public service information security in the context of big data,” in *Proceedings of the 2020 2nd International Conference on Big Data and Artificial Intelligence*, Apr. 2020, pp. 86–92, doi: 10.1145/3436286.3436304.

[18] A. B. Setiawan, "In the application of E-Government," (in Bahasa), *Jurnal Masyarakat Telematika dan Informasi*, vol. 4, no. 2, pp. 109–126, 2013.

[19] E. Prima, R. Lumanto, and Z. A. Hasibuan, "Evaluation of government public key infrastructure implementation based on eGovAMAN framework," Department Homeland University, Carnegie Mellon University, 2013.

[20] E. Prima, Y. G. Sucahyo, and Z. A. Hasibuan, "Mapping the certification authority for e-government procurement system into eGovAMAN framework," in *International Conference on Advanced Computer Science and Information Systems (ICACSIS)*, Sep. 2013, pp. 61–65, doi: 10.1109/ICACSIS.2013.6761553.

[21] DHS, *State cybersecurity governance case studies*. Department of Homeland Security National Association of State Chief Information Officers, 2017.

[22] DHS, "*Cyber resilience review*," Department Homeland University, Carnegie Mellon University, 2011.

[23] A. Jamil and Z. M. Yusof, "Information security governance framework of Malaysia public sector," *Asia-Pacific Journal of Information Technology and Multimedia*, vol. 7, no. 2, pp. 85–98, Dec. 2018, doi: 10.17576/apjitm-2018-0702-07.

[24] S. Perumal, S. Ali Pitchay, G. Narayana Samy, B. Shanmugam, P. Magalingam, and S. Hasan Albakri, "Transformative cyber security model for Malaysian government agencies," *International Journal of Engineering and Technology*, vol. 7, Oct. 2018, doi: 10.14419/ijet.v7i4.15.21377.

[25] S. N. Deekue, "A strategic framework for e-government security: the case in Nigeria," University of Bedfordshire, 2016.

[26] J. van't Wout, M. Waage, H. Hartman, M. Stahlecker, and A. Hofman, *The integrated architecture framework explained*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, doi: 10.1007/978-3-642-11518-9.

[27] B. Rahardjo, *Information & network security*, (in Bahasa), Bandung: PT Insan Infonesia, 2017.

[28] Y. Li, T. Stafford, B. Fuller, and S. Ellis, "Information securing in organizations," in *Proceedings of the 2019 on Computers and People Research Conference*, Jun. 2019, pp. 125–130, doi: 10.1145/3322385.3322425.

[29] A. B. Setiawan, A. Syamsudin, and A. S. Sastrosubroto, "Information security governance on national cyber physical systems," in *International Conference on Information Technology Systems and Innovation (ICITSI)*, Oct. 2016, pp. 1–6, doi: 10.1109/ICITSI.2016.7858210.

[30] S. AlGhamdi, K. T. Win, and E. Vlahu-Gjorgievska, "Information security governance challenges and critical success factors: systematic review," *Computers and Security*, vol. 99, Dec. 2020, doi: 10.1016/j.cose.2020.102030.

[31] G. Gashgari, R. Walters, and G. Wills, "A proposed best-practice framework for information security governance," in *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security*, 2017, pp. 295–301, doi: 10.5220/0006303102950301.

[32] R. von Solms and J. van Niekerk, "From information security to cyber security," *Computers and Security*, vol. 38, pp. 97–102, Oct. 2013, doi: 10.1016/j.cose.2013.04.004.

[33] Capgemini, "Information security benchmark 2019," *Research Report*, 2019.

[34] BSSN, *KAMI Index Version 4.0*, (in Bahasa), Indonesia Security Guideline Document, 2019.

[35] F. Setiadi, A. Rubhasy, and Z. A. Hasibuan, "Identifying and validating components for national cyber security framework," in *Third International Conference on Informatics and Computing (ICIC)*, Oct. 2018, pp. 1–5, doi: 10.1109/IAC.2018.8780441.

[36] Y. Nugraha, "The future of cyber security capacity in Indonesia," Indonesian Institute of Sciences, 2016.

[37] E. K. Szczepaniuk, H. Szczepaniuk, T. Rokicki, and B. Klepacki, "Information security assessment in public administration," *Computers and Security*, vol. 90, Mar. 2020, doi: 10.1016/j.cose.2019.101709.

[38] J. Zuo, Y. Lu, H. Gao, R. Cao, Z. Guo, and J. Feng, "Comprehensive information security evaluation model based on multi-level decomposition feedback for IoT," *Computers, Materials and Continua*, vol. 65, no. 1, pp. 683–704, 2020, doi: 10.32604/cmc.2020.010793.

[39] K. Prislan, A. Mihelič, and I. Bernik, "A real-world information security performance assessment using a multidimensional socio-technical approach," *PLoS ONE*, vol. 15, Sep. 2020, doi: 10.1371/journal.pone.0238739.

[40] M. Gulzira, B. Gulmira, S. Altynbek, and O. Assel, "The audit method of enterprise's Information security," in *Proceedings of the 6th International Conference on Engineering*, Sep. 2020, pp. 1–5, doi: 10.1145/3410352.3410761.

[41] V. Monev, "Organisational information security maturity assessment based on ISO 27001 and ISO 27002," in *International Conference on Information Technologies (InfoTech)*, Sep. 2020, pp. 1–5, doi: 10.1109/InfoTech49733.2020.9211066.

[42] D. Sulistyowati, F. Handayani, and Y. Suryanto, "Comparative analysis and design of cybersecurity maturity assessment methodology using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS," *JOIV: International Journal on Informatics Visualization*, vol. 4, no. 4, Dec. 2020, doi: 10.30630/joiv.4.4.482.

[43] A. Erulanova, G. Soltan, A. Baidildina, M. Amangeldina, and A. Aset, "Expert system for assessing the efficiency of information security," in *7th International Conference on Electrical and Electronics Engineering*, Apr. 2020, pp. 355–359, doi: 10.1109/ICEEE49618.2020.9102555.

[44] T. Tagarev and D. Polimirova, "Main considerations in eclaborating organizational information security policies," in *Proceedings of the 20th International Conference on Computer Systems and Technologies*, Jun. 2019, pp. 68–73, doi: 10.1145/3345252.3345302.

[45] S. E. Change, A. Y. Liu, and Y.-T. J. Jang, "Exploring trust and information monitoring for information security management," in *10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI)*, Oct. 2017, pp. 1–5, doi: 10.1109/CISP-BMEI.2017.8302319.

[46] V. G. Eryshov and D. V. Ilina, "Method of the information security monitoring process in information and telecommunication systems based on the application of methods of markov random processes," in *Wave Electronics and its Application in Information and Telecommunication Systems (WECONF)*, Jun. 2020, pp. 1–4, doi: 10.1109/WECONF48837.2020.9131492.

[47] F. Ö. Sönmez, "A conceptual model for a metric based framework for the monitoring of information security tasks' efficiency," *Procedia Computer Science*, vol. 160, pp. 181–188, 2019, doi: 10.1016/j.procs.2019.09.459.

[48] J. Andress, *Foundations of information security*. No Starch Press, 2019.

[49] A. AlKalbani, H. Deng, B. Kam, and X. Zhang, "Information security compliance in organizations: an institutional perspective," *Data and Information Management*, vol. 1, no. 2, pp. 104–114, Dec. 2017, doi: 10.1515/dim-2017-0006.

[50] M. Lubis, R. Fauzi, P. Liandani, and A. R. Lubis, "Information security awareness (ISA) towards the intention to comply and demographic factors: statistical correspondence analysis," in *Proceedings of the 8th International Conference on Computer and Communications Management*, Jul. 2020, pp. 79–84, doi: 10.1145/3411174.3411196.

[51] J. Vacca, *Computer and information security handbook*, 3rd ed. Morgan Kaufmann, 2013, doi: 10.1016/C2011-0-07051-5.

[52] M. Asgarkhani, E. Correia, and A. Sarkar, "An overview of information security governance," in *International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET)*, Feb. 2017, pp. 1–4, doi: 10.1109/ICAMMAET.2017.8186666.

[53] H. Paananen, M. Lapke, and M. Siponen, "State of the art in information security policy development," *Computers and Security*,

vol. 88, Jan. 2020, doi: 10.1016/j.cose.2019.101608.

[54] J. Lobo, E. Bertino, and A. Russos, "On security policy migrations," in *Proceedings of the 25th ACM Symposium on Access Control Models and Technologies*, Jun. 2020, pp. 179–188, doi: 10.1145/3381991.3395613.

[55] W. Jatmiko *et al.*, *Scientific article writing*, (in Bahasa), Depok: UI Publishing, 2015.

[56] M. N. Masrek, Q. N. Harun, and M. K. Zaini, "Information security culture for Malaysian public organization: a conceptual framework," in *4th International Conference on Education and Social Sciences (Intcess 2017)*, pp. 156–166, 2017.

BIOGRAPHIES OF AUTHORS

Rika Yuliana completed her master's level study in Informatics Engineering at the Bandung Institute of Technology in 2012 and bachelor's degree in Agro-Industrial Technology at the Bogor Agricultural University in 2006. Currently she is actively involved as a teaching staff and researcher at the Faculty of Science and Technology (FST) of the State Islamic University (UIN) Ar-Raniry Banda Aceh. The research fields carried out include information technology governance and architecture in both corporate and government organizations. She can be contacted by email: rika.yuliana@ar-raniry.ac.id.

Zainal Arifin Hasibuan was born in Pekan Baru, Indonesia in 1959. He received B.Sc. degree in Statistic from Bogor Institute of Agriculture, Indonesia, 1986, M.Sc. and Ph.D. in Information Science, Indiana University, in 1989 and 1995 respectively. Currently, he is a lecturer and Ph.D. supervisor at Faculty of Computer Science, University of Indonesia. He is also the Head of Digital Library and Distance Learning. His research interests include e-learning, digital library, information retrieval, information system, and software engineering. He can be contacted by email: zhasibua@dsn.dinus.ac.id.