University of Southampton

Faculty of Engineering and Physical Science

School of Electronics and Computer Science

Information Assurance Framework for eGovernment in Indonesia

By

Rio Guntur Utomo

ORCID ID 0000-0002-7358-5316

Supervisors: Dr Gary B. Wills and Dr Robert J. Walters

Thesis for the degree of Doctor of Philosophy in Computer Science

April 2020

Dedication Page

I dedicate this thesis to my family

for their constant support and unconditional love.

I love you all dearly.

University of Southampton

Abstract

Faculty of Engineering and Physical Science

School of Electronics and Computer Science

Thesis for the degree of Doctor of Philosophy in Computer Science

Information Assurance Framework for eGovernment in Indonesia

By

Rio Guntur Utomo

Information technology has been used in various fields, such as business, health, and education. This includes in government field, which is often called electronic government or eGovernment. In fact, many countries had implemented eGovernment, including Indonesia. The eGovernment initiative is aimed to improve government services to the public by improving the quality and availability of services that can be accessed regardless of time and place. Consequently, the services must always be available at any time, and any threat to the information and systems should receive attention to ensure business continuity in the event of an incident. However, in Indonesia, the implementation of eGovernment is still unsatisfying according to the United Nations eGovernment Development Index 2018. One of the reasons, as stated by the Director of eGovernment of Ministry of Communication and Information of Indonesia, is the information security aspect of eGovernment in Indonesia is still relatively vulnerable. Therefore, in the implementation of eGovernment, information assurance (IA) should be considered.

The main purpose of IA is to protect the business by reducing risks associated with information and information systems as well as ensuring business continuity. However, there is no study so far that has focused on IA for eGovernment in Indonesia. For this reason, research on a framework of IA is needed to support the implementation of eGovernment in Indonesia. This research focuses on the development of an IA framework for eGovernment within the Indonesian context.

The development of the framework is divided into four stages, which are identifying the factors from international best practices for IA, determining factors from literature, identifying the challenges, and evaluating and harmonising all the factors. The proposed framework is expected to assist eGovernment implementation in Indonesia to achieve eGovernment initiatives in Indonesia. The framework confirmed using the triangulation method by conducting a literature review, experts' interview, and survey with practitioners in the field of IA, eGovernment, and information security from various institutions in Indonesia.

The findings show that all the proposed factors in the framework are significant in IA implementation for eGovernment in Indonesia. Moreover, an instrument to measure IA implementation status derived from the confirmed framework was developed and validated. The results show that the instrument is able to assess accurately the status of IA implementation in government organisations in Indonesia and therefore it can be concluded that the framework is feasible to be implemented in Indonesia.

Table of Contents

Table of Tables

Table of Figures

Research Thesis: Declaration of Authorship

Print name: Rio Guntur Utomo

Title of thesis: Information Assurance Framework for eGovernment in Indonesia

I declare that this thesis and the work presented in it are my own and has been generated by me as the result of my own original research.

I confirm that:

1. This work was done wholly or mainly while in candidature for a research degree at this University;
2. Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated;
3. Where I have consulted the published work of others, this is always clearly attributed;
4. Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work;
5. I have acknowledged all main sources of help;
6. Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself;
7. Parts of this work have been published as:
    - R. G. Utomo, R. J. Walters and G. B. Wills, "Factors affecting the implementation of information assurance for eGovernment in Indonesia," *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)*, Cambridge, 2017, pp. 225-230. DOI: 10.23919/ICITST.2017.8356388
    - R. G. Utomo, G. B. Wills and R. J. Walters, "Towards Confirming an Information Assurance Framework for eGovernment in Indonesia," *2018 International Conference on ICT for Smart Society (ICISS)*, Semarang, 2018, pp. 1-6. DOI: 10.1109/ICTSS.2018.8550010
    - R. G. Utomo, G. B. Wills and R. J. Walters, "Investigating Factors in Information Assurance Implementation: Towards Developing an Information Assurance Framework for eGovernment in Indonesia," *2018 International Conference on Information Technology Systems and Innovation (ICITSI)*, Bandung - Padang, Indonesia, 2018, pp. 10-15. DOI: 10.1109/ICITSI.2018.8695932

Signature: Date: 14/04/2020

Acknowledgements

I would like to thank my supervisors, Dr Gary Wills and Dr Robert Walters, for supporting me during these past three and a half years, and also for the patient guidance, encouragement, and advice they have provided throughout my time as their student. I have been extremely grateful to have supervisors who cared so much about my work, and who responded to my questions and queries so promptly.

I also would like to thank my examiners, Professor Mike Wald, Dr Andy Gravell, and Dr Nick Savage for their constructive suggestions, which were determinant for the accomplishment of the work presented in this thesis.

I also thank my family for their support and my parents for all they have done for me over the years. I couldn't have achieved any of this without their support and guidance. Their prayer for me was what sustained me this far.

To my wife, Chelsea, for her patience, motivation, encouragement, and unconditional support.

To my close friends, especially my housemates, I express my gratitude for their friendship, support, and patience throughout these years.

To my colleagues and friends of the Cyber-Physical System Group in the School of Electronics and Computer Science, I thank them for their companionship and for providing a so pleasurable and friendly working atmosphere.

I acknowledge the financial support for my research study of the Indonesia Endowment Fund for Education (Lembaga Pengelola Dana Pendidikan) through the Doctoral scholarship.

Definitions and Abbreviations

CCEB	Combined Communications Electronics Board
CESG	Communications-Electronics Security Group
COBIT	Control Objectives for Information and Related Technologies
CPNI	Centre for the Protection of National Infrastructure
CSIA	Central Sponsor for Information Assurance
DOD	Department of Defense
DTI	Department of Trade and Industry
G2B	Government-to-Business
G2C	Government-to-Citizen
G2E	Government-to-Employee
G2G	Government-to-Government
G2N	Government-to-Non-profit
GCHQ	UK Government Communications Headquarters
IA	Information Assurance
IASME	Information Assurance for Small and Medium Enterprises
InfoSec	Information Security
ISMS	Information Security Management Standards
ISO/IEC	International Organization for Standardization and the International Electrotechnical Commission
MICT	Ministry of Information and Communications Technology
OECD	Organisation for Economic Co-operation and Development
PAS	Publicly Available Specification
SANS	SysAdmin, Audit, Network, and Security

Chapter 1 **Introduction**

In the modern world, technology is an integral part of everyday life and cannot be separated from progress and human development (World Bank, 2008) and from everyday life (OECD, 1998). Moreover, the use of digital technology has given rise to a new mechanism of government bureaucracy which is then known as the Electronic Government (eGovernment) (Indrajit, 2006). The World Bank (2015) defines eGovernment as the use of information technologies (such as wide area network, the Internet, and mobile computing) by government agencies that could transform relations with citizens, business, and other government organisations. The shift towards eGovernment was aimed at introducing changes to the traditional approach of public service delivery. In fact, several governments have become increasingly aware of the benefits of eGovernment in improving the performance of government organisations and their interactions with their citizens (Ebrahim & Irani, 2005). One of the governments that had implemented eGovernment is Indonesia.

Indonesia is the largest archipelago in the world with the number of islands reached more than 17,000. This geographic condition becomes one of the reasons for the government to implement eGovernment. In this case, it is argued that based on the geographical challenges it faces, there are 5 reasons why the Indonesian government needs to implement eGovernment (Dahlan, 2008), those are: to support the government changes towards democratic governance, to support the application of balances authority between central and local Governments, to facilitate communication between central and local government, to gain openness, to facilitate the transformation towards an information society era. In addition, the term eGovernment in Indonesia refers to the use of information technology (IT) in the service procedures organised by government organisations (Sipatuhar & Sutaryo, 2016).

Implementation of eGovernment provides many advantages, such as improved quality of service in which eGovernment systems allow public, business, and government sectors to have access 24 hours a day, seven days a week to government information (Ndou, 2004). Reduced costs and process levels in organisations have streamlined the operational procedures, which are also benefits from the implementation of eGovernment (Seifert, 2003). In addition, the performance of government agencies in providing public services to customers will be more effective and efficient (Hwang & Rubin, 2004). Besides, the implementation of eGovernment will also increase the transparency and service to the public, improve service and efficiency, reduce transaction costs, and provide benefits from an economic perspective (Cohen & William, 2002).

Furthermore, in Indonesia, the implementation of eGovernment initiatives began with the publication of the Presidential Instruction No. 3 in 2003 (Presiden Republik Indonesia, 2003). However, the index and evaluation of eGovernment implementation in Indonesia have not shown satisfactory results. Based on data released by the UN (United Nations, 2018), Indonesia currently is ranked 107th out of 193 countries assessed by the UN EGDI (eGov Development Index) for Indonesia is 0.5258, the index is still below the average value EGDI for all countries assessed is 0.5491.

Moreover, the Director of eGovernment of Ministry of Communication and Information of Indonesia states that in line with the increasing number of information presented by the government as part of the service, the greater the challenges of information security are also increasing, and according to their study, the information security aspect of eGovernment in Indonesia is still relatively vulnerable (Hukum Online, 2014). In addition, there are also other problems regarding eGovernment implementation as stated by some literature. The availability of services has become a significant concern (Jaeger & Thompson, 2003). Further, according to Basu (2004), assurance of the security of the communications and its sources has also become an issue. Users are mainly concerned about the integrity of the communicated information. In addition, with eGovernment reliance on information systems and services, it is more vulnerable to threats and needs to be protected (ISO/IEC 27001:2013, 2013). To overcome this problem, information assurance (IA) is needed as a mechanism to protect information systems and services.

Information assurance (IA) is still related to information security (InfoSec). IA is about the protection of information assets from destruction, degradation, manipulation, and exploitation, this includes providing restoration of information systems (Blyth & Kovacich, 2006). Meanwhile, the purpose of InfoSec is to prevent and minimise the effects of security incidents (Liu et al., 2006). Additionally, InfoSec operates by sustaining and defending confidentiality, integrity, and availability, which are the three critical security properties (May, 2006). However, as information is shared in the implementation of eGovernment, more layers of properties should be taken into consideration, there are identification, authentication, accountability, non-repudiation, authorisation, and privacy (May, 2006). Therefore, since InfoSec is more focused on the confidentiality, integrity, and availability, alternatively, it is necessary to implement IA instead, which has a strong emphasis on strategic risk management and has a broader connotation that includes reliability, authentication, and non-repudiation (Hibbard, 2009). Moreover, IA also provides restoration of information systems by combining protection, detection, and reaction capabilities (May, 2006).

The main purpose of IA is to protect the business by reducing risks associated with information and information systems (Hibbard, 2009). The activity is driven by risk analysis and cost-effectiveness

with comprehensive and systematic management of security countermeasures (Cherdantseva & Hilton, 2013). Additionally, IA relies on multiple, related, organisational actions and controls in the form of the defence in depth model (May, 2006). All IA processes are carried out to support corporate governance (Rathmell et al., 2004). With services and business continuity are assured, it is expected that the eGovernment services will be implemented successfully; therefore, the purpose of implementation of eGovernment will be achieved, which is to improve the effectiveness, efficiency, and quality of service to the citizens.

Therefore, to implement eGovernment in Indonesia successfully, the IA of eGovernment in Indonesia requires attention. Hence, the aim of this research is to develop a framework of IA to support to the implementation eGovernment in Indonesia.

1.1 Peer-reviewed contributions

R. G. Utomo, R. J. Walters and G. B. Wills, "Factors affecting the implementation of information assurance for eGovernment in Indonesia," *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)*, Cambridge, 2017, pp. 225-230. DOI: 10.23919/ICITST.2017.8356388

R. G. Utomo, G. B. Wills and R. J. Walters, "Towards Confirming an Information Assurance Framework for eGovernment in Indonesia," *2018 International Conference on ICT for Smart Society (ICISS)*, Semarang, 2018, pp. 1-6. DOI: 10.1109/ICTSS.2018.8550010

R. G. Utomo, G. B. Wills and R. J. Walters, "Investigating Factors in Information Assurance Implementation: Towards Developing an Information Assurance Framework for eGovernment in Indonesia," *2018 International Conference on Information Technology Systems and Innovation (ICITSI)*, Bandung - Padang, Indonesia, 2018, pp. 10-15. DOI: 10.1109/ICITSI.2018.8695932

1.2 Report structure

The remainder of this report is structured as follows. The research report is divided into eight chapters. Chapter 2 presents a literature review, which illustrates the concepts of eGovernment, information security, IA, the importance of IA, followed by IA standard-based frameworks, IA factors and challenges. Chapter 3 presents the proposed framework and the description of the framework development and its components. Chapter 4 discusses the research methodology for this research. Chapter 5 presents findings, results, and discussions of the validation phase of the framework. Chapter 6 presents the development and validation of the instrument. Chapter 7

discusses findings, results, and discussions of the case studies. Chapter 8 is the conclusion of this report. In addition, the chapter also presents a plan for future work.

Chapter 2 **Literature review**

This chapter provides the context for the present work. It gives an overview of the concept of eGovernment, Information Security (InfoSec) and Information Assurance (IA). In addition, it shows why InfoSec alone is not enough in providing assurance of information, but also needs IA, and defines the relationship between both approaches. This chapter also clarifies the status of eGovernment in Indonesia, the global IA frameworks, and the approaches that stressed factors for effective IA implementation.

2.1 eGovernment

The term eGovernment is defined as a way for the government to use technologies to benefit citizens and businesses with improved quality access to government information and services to be more efficient, effective, convenient, and accountable (Fang, 2002; Khalil, Lanvin & Chaudhry, 2002; World Bank, 2015). For the purpose of this study, it can be concluded that eGovernment is the use of technologies to enhance government services to benefit citizens, business partners, and employees.

Furthermore, the main purpose of eGovernment is to serve the citizens and facilitate interaction between citizens and the government, which also makes public information more accessible with the use of IT and reduces the time and costs incurred when making transactions (Ndou, 2004). Additionally, eGovernment aims to create a better business environment, to strengthen good governance by expanding public participation, and to improve government productivity and efficiency by streamlining operational procedures (Yanqing, 2010).

In providing services to the public, eGovernment combines aspects of technology, business processes, and human resources (Silcock, 2001). The use of Internet-based applications is intended to make access to information easier and more convenient for citizens and businesses, to improve the quality of services, and to increase participation in democratic institutions and processes (Yanqing, 2010). In addition, eGovernment enhances and updates internal systems and procedures that will improve government processes, cost-cutting, performance, effectiveness, and inter-governmental relationships (Yanqing, 2010).

Moreover, eGovernment should focus on five consumer-to-government relationships: government-to-government (G2G), government-to-citizen (G2C), government-to-business (G2B), government-to-employee (G2E), and government-to-nonprofit (G2N) (Fang, 2002). In addition, G2G refers to the relationship between the government using online communication between

government organisations, departments, and agencies (Curtin, 2007). Relating to the relationship between government and business, G2B primarily deals with the procurement of products and services (Fang, 2002), which are offered through a significant role in the development of business, especially small and medium enterprises (SMEs; Joseph, 2009). Covering the relationship between the government and citizens, G2C gives citizens access to government information and communications through online services (Fang, 2002). Lastly, G2E facilitates internal communication between government employees and provides management of civil services, while G2N provides information and communication to nonprofit organisations (Fang, 2002).

The key reason for the importance of eGovernment is the influence of Internet development as a global networking and communication system that links the state, economy, and citizens, which makes the Internet an ideal technology for interacting and collaborating with all types of public stakeholders (Wirtz & Daiser, 2015).

The benefits of eGovernment include providing broad access to government information, promoting interaction between the public and government officials, making the government more accountable and transparent, while reducing opportunities for corruption, and providing development opportunities, especially for rural and traditionally underserved communities (Khalil, Lanvin & Chaudhry, 2002).

Besides benefits, eGovernment also has challenges in its implementation. According to Jaeger and Thompson (2003), with the reliance of eGovernment services on the web, the availability of services becomes an important concern. There should be a necessary level of telecommunication infrastructure required and minimum standards of ability to access the services offered. The issue of assurance as to the security of the communications and its sources is also a concern (Basu, 2004). Each user will focus on the integrity of the communicated information and the trustworthiness and whether it has been altered after it was sent. Moreover, Alateyah (2012) listed trust, privacy, security, computer and information literacy, culture, authentication, technical infrastructure, accessibility, availability, and eGovernment services adoption as the most common barriers to the implementation of eGovernment.

2.2 Information security

In the era of high technology, organisations have become more dependent on their information systems. In line with the rise of crime against information systems, organisations identify information as an area that should be protected as part of their internal control systems (Turnbull,

2003). Information security (InfoSec) protects information and facilities that store, use, and transmit data from a wide range of threats to keep its value to the organisation (DTI, 2006).

The universal definition of InfoSec is the confidentiality, integrity, and availability of information (Kociemba, 2015). Confidentiality means that information should stay secret and only be accessible to the person with authority (Ezingeard et al., 2005). Trustworthiness, origin, completeness, and correctness become the concerns of integrity (May, 2006). Availability deals with the availability of information to authorised users when they need it (Kociemba, 2015).

The three elements of confidentiality, integrity, and availability are the foundations of information security (May, 2006). However, as information is shared and exchanged, more concern must be given to other layers, such as the following:

- accountability to determine the actions and behaviour of users,
- non-repudiation, which is the mechanism that keeps individuals from denying their actions, (May, 2006; Hibbard, 2009).

If one of these layers is not achieved, then the confidentiality, integrity, and availability will be lost (May, 2006). It means InfoSec alone is not enough in providing assurance of information. Therefore, an additional mechanism is needed that can assure and protect information when it is being shared or exchanged. IA is an approach that is based on confidentiality, integrity, and availability. By making InfoSec its centre, IA is activating all security mechanisms and effectively managing all processes of processing, conveying, and storing information (Yalman & Yesilyurt, 2013). In addition, IA also provides restoration of information systems by combining the protection, detection, and reaction capabilities (May, 2006).

2.3 Information assurance

The U.S. Department of Defense (DOD) defines IA as actions that secure information and information systems by ensuring their availability, integrity, authentication, confidentiality, non-repudiation, and providing for restoration of information systems (U.S. Department of Defense (DOD), 2007). Moreover, the UK Government's Central Sponsor for Information Assurance (CSIA) in their National Information Assurance Strategy defines IA as confidence in the processes of information risk management and IA should assure the availability, integrity, confidentiality, non-repudiation and authentication of information and information systems (CSIA, 2007). Further, another definition describes IA as the protection of information assets from destruction, degradation, manipulation, and exploitation, this includes providing restoration of information systems (Blyth & Kovacich, 2006). Therefore, from the definitions, for the purpose of this study, it

can be concluded that IA is defined as operations that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, non-repudiation and providing for restoration of information systems.

Compared to information security, IA has a wider scope. In general, InfoSec focuses more on protection and prevention, whereas the focus of IA is more on the integration of protection, detection, and reaction (Liu et al., 2006). InfoSec itself is more focused on the confidentiality, integrity, and availability, while IA, which has a strong emphasis on strategic risk management, has a broader connotation that includes reliability, authentication, and non-repudiation (Hibbard, 2009).

In addition, IA is constructed by the defence in depth that applies organisational actions and control to minimise failure and intrusion (May, 2006). Defence in depth is an approach that integrates the capabilities of personnel, operations, and technology to achieve IA (U.S. Department of Defense (DOD), 2002). By adopting defence-in-depth, IA includes several aspects in its concepts, such as risk management; training, education, and professionalism of staff; programmes and issue- and system-specific policies; monitoring, management, and administration; and assessment and audit (US Joint Staff, 2000).

The IA process is iterative and aims for continuous improvement, starting with enumerating and classifying information assets, followed by risk assessment. These processes assess the vulnerabilities and threats that could affect the information. After risk assessment, the next step is risk analysis. This step analyses the likelihood of effects of the risk to the information. The next process is risk management, which focuses on the treatment of the risk. Afterwards, testing and review are the final stages, which are then repeated for continual improvement (Hibbard, 2009).

The focus of IA is reducing risks associated with information, which can assure business continuity by considering both organisational and human aspects (Blyth & Kovacich, 2006). However, IA cannot be separated from information security, which complements IA by dealing with the protection of information and technical countermeasures.

2.4 Importance of information assurance

The IA strategy can ensure reliability, accuracy, security, and availability of information assets in line with corporate goals and strategies for maximum benefits for the organisation (Ezingeard et al., 2005). In addition, IA also provides benefits by ensuring business continuity by reducing risks associated with information and information systems (Cherdantseva & Hilton, 2013).

Benefits of the implementation of IA in the organisation are not merely related to the business continuity scale. Further advantages of the IA implementation include operational, tactical, strategic, and organisational aspects (Ezingeard et.al, 2005). Moreover, IA is a key to realising reliable management decision making, customer trust, business continuity, and good governance, which is critical for organisations in all sectors of industry and public service (Ezingeard et al., 2005).

For eGovernment, the implementation of IA will affect the achievement of eGovernment goals and objectives by providing the requirement of integrity and availability, which then implies the improved ability to deliver products and services online (Bowen & Hash, 2007).

2.5 eGovernment in Indonesia

Indonesia officially began implementing eGovernment with the publication of the Republic of Indonesia Presidential Instruction No. 3 of 2003. The development of eGovernment is an effort to implement electronic-based governance to improve the quality of public services effectively and efficiently. Through the development of eGovernment, management systems and processes carried out in the government environment are restructured by optimising the utilisation of IT. The utilisation of IT includes two related activities (Presiden Republik Indonesia, 2003), among others:

(1) IT advances for public services can be accessed easily and cheaply by citizens throughout the country;

(2) Data processing, information management, systems management, and work processes are done electronically.

Since 2003, there has been a steady increase in local government capability in using and managing IT for their eGovernment initiative. A successive survey by the Ministry of Communication and Informatics in 2009 and 2011 showed a 3.7% increase in the eGovernment rating of provincial governments (Kominfo, 2010, 2012). Eight provincial governments were awarded with an “adequate” label in 2011, compared to only four provinces in 2009. As of 2013, 11 provincial government have been awarded the "adequate" label.

A survey in 2014 on eGovernment implementation in local governments within the West Java province also shows promising figures on the capability of local government. While there is evidence of the lack of IT-governance implementation, the basic IT capacity is adequate, which means most of them are capable enough to be able to implement eGovernment to provide online services to the public:

- 100% have an official website;
- 63% have a dedicated server room;
- 67% have or operate on multisite closed networking;
- 83% own an administrative web application; and
- 46% run some form of public service website.

According to the eGovernment roadmap of Indonesia (Anggono, 2015), until 2014, the eGovernment system development was still in the form of silos. Furthermore, from 2015 to 2018, eGovernment systems and national eGovernment infrastructures were being integrated. The year 2019 will begin the optimisation era, where services like G2G, G2B, G2C, and G2E will begin to be implemented. According to Karokola (2012), eGovernment service security is often not considered at the initial stages, and it is argued that it should be considered from the initial stage of information systems, IT, and information and communication technology (ICT) development for eGovernment services. It is expected that the development of a framework that focuses on IA for eGovernment in Indonesia can be helpful in the development of eGovernment services in Indonesia.

2.6 International Best Practices for IA

The most recent and well-known IA industrial best-practice frameworks are IASME, ISO/IEC 27001, and COBIT 5 for Assurance.

In 2011, the IASME Consortium published the IASME document aimed at providing guidance on SMEs to assess and acknowledge the level of maturity of their business information security. The processes are adopted from international standards and EU guidelines, which are simple, fast, and cost-effective. The advantage of IASME is that this standard can be adjusted with other standards, such as ISO/IEC 27001, Publicly Available Specification (PAS) 555, Communications-Electronics Security Group (CESG) 10 Steps to Cyber Security, and Centre for the Protection of National Infrastructure (CPNI)/SysAdmin, Audit, Network, and Security (SANS) 20 Critical Controls for Cyber Defence.

In addition, IASME works by applying control sets to all business types and adjusting their implementation regarding the business risk profile. Although developed for smaller businesses, the IASME process can now be adapted to any business size. For effective implementation, IASME is based on 12 factors for its guidance (IASME, 2013). The 12 factors are the following:

1. Organisation
2. Risk
3. Policy and Compliance

4. Assets
5. Planning
6. Access
7. People
8. Physical and Environmental
9. Disruption
10. Operations
11. Incident Management
12. Continuity

Furthermore, the International Organisation for Standardization (ISO) and International Electrotechnical Commission (IEC) standard (ISO/IEC 27001: 2013), Information Assurance for Small and Medium Enterprises (IASME), and Control Objectives for Information and Related Technologies (COBIT) 5 are three best practice standard-based frameworks that have been developed and recognised internationally. Although ISO/IEC 27001 is intended for ISMS, according to Hibbard (2009) ISO/IEC 27001: 2013 is more closely aligned with information assurance (IA).

The standard ISO/IEC 27001 was originally developed as British Standard 7799 by BSI Group, which later adopted by ISO as ISO/IEC 27001 in 2005. This standard provides guidelines for establishing, implementing, maintaining, and continually improving information security management systems. The standard states that the purpose of ISMS is to manage and control information security risk and to protect and maintain confidentiality, integrity, and availability. The standard also identifies the outcomes of an effective ISMS implementation, which are adequate control over information security, good governance in handling and securing information, and having a mechanism for measuring the success or absence of security control.

The standard also has guidelines for integrating ISMS with organisational strategies based on seven key requirements (ISO / IEC 27001, 2013). The seven requirements are the following:

1. Context of the organisation
2. Leadership
3. Planning
4. Support
5. Operation
6. Performance evaluation
7. Improvement

Moreover, COBIT 5 is a framework of principles, practices, analytical tools, and models that are globally accepted and can help in identifying critical business issues related to governance and management of information and technology for enterprises. The COBIT 5 for Assurance focuses on defining assurance objectives that align with enterprise objectives by maximising the value of assurance initiatives (COBIT 5, 2013). In addition, COBIT 5 provides guidance for establishing and sustaining assurance for enterprises and provides a structured approach on how to provide assurance over enablers.

The scope of COBIT 5 for Assurance consists of two perspectives, namely, the assurance function perspective that describes what is needed in building and the assurance and assessment perspective functions that describe which assurance needs to be provided. These two perspectives are built on the seven-common governance and management enablers of the COBIT 5 framework (COBIT 5, 2013), which are as follows:

1. Processes
2. Organisational Structures
3. Culture, Ethics, and Behaviour
4. Principles, Policies, and Frameworks
5. Information
6. Services, Infrastructure, and Applications
7. People, Skills, and Competences

Key factors for successful implementation from the IA industrial best-practice frameworks were identified and analysed to determine the concept. Furthermore, some factors have similarities in concept; these factors were removed to avoid duplication. The factors are summarised into Table 2.1. Although these factors are from international best practices, it is still necessary to identify other factors from relevant literature that are expected to complement IA aspects that are not covered by the best practices.

Table 2.1 Summary of factors from IA industrial best-practice frameworks

Factors	IASME	ISO/IEC 27001	COBIT 5
Access Control	√		
Awareness	√	√	
Communication		√	
Competence	√	√	√
Continual improvement		√	
Culture, Ethics and Behaviour			√
Disaster Recovery/Business Continuity	√	√	
Information		√	√
Information security		√	
Internal audit		√	√
Leadership and commitment		√	
Malware and technical intrusion	√		
Management review		√	
Monitoring, measurement, analysis and evaluation	√	√	
Operational planning and control		√	
Operations and Management	√		
Organizational roles, responsibilities and authorities	√	√	√
Physical and Environmental Protection	√		
Policy and Compliance	√	√	√
Resources		√	
Processes			√
Risks and opportunities	√	√	
Services, Infrastructure and Applications			√

2.7 IA factors

According to Bullen and Rockart (1981), critical success factors (CSFs) are a limited number of areas that must be met and implemented properly for the organisation to achieve its goals and objectives. A good implementation of CSFs will ensure the successful performance of an individual, department, or organisation (Bullen & Rockart, 1981). In IA, success in implementation means there is no data breach and also the integrity and availability of services are guaranteed. For the purpose of this study, the CSFs for IA from the literature will be addressed as IA factors.

There are several studies on the factors in IA implementation within organisations. Bunker (2012), stated in their study that the business strategy and strategic direction of the organisation affect IA. Moreover, IA is often only considered a technical problem, but in practice, IA should be approached holistically, which is connected to business and strategy.

Cherdantseva and Hilton (2013), published a reference model of information assurance and security (RMIAS). This model conveys a perception of IA as a complex organisational and managerial concern

and requires comprehensive and systematic treatment. The model also listed security countermeasures in implementing IA and security, which are focused on organisational, technical, legal, and human-oriented aspects.

The Ministry of Information and Communications Technology (MICT, 2014), which is a Qatari Ministry, published a National Information Assurance Policy (NIASP) that can be used in all sectors. The NIASP presents the necessary and relevant foundation for implementing an ISMS in the organisation. According to MICT, key factors in protecting information are awareness and education for users and employees, as they are the users and managers of that information.

The Combined Communications Electronics Board (CCEB) published 'Information Assurance for Allied Communications and Information Systems' (CCEB, 2015), which was intended for the five-member nations of Australia, Canada, New Zealand, the United Kingdom, and the United States. The document listed IA principles as well as components and defines the IA policies and procedures to enable a secure combined information environment.

A group within the UK Government Communications Headquarters (GCHQ), CESG, published 'The Information Assurance Maturity Model and Assessment Framework' (CESG, 2015). The IAMM consists of five levels with three main IA goals. The key process for the IA goals are leadership and governance; training, education, and awareness; information risk management; through-life IA measures; assured information sharing; and compliance. For organisations, these processes facilitate achieving the maturity to accomplish trust in the information systems and processes, both internally and between organisations.

Chris Cope, the lead auditor of ISO27001 and a CESG certified professional, listed principles for effective IA (Cope, 2015). The principles are intended to enhance the security of any organisation. The principles have a strong emphasis on business alignment, a holistic and risk-driven approach, and good governance within a less policy-constrained environment, as CESG withdrew the mandatory requirement to use Information Assurance Standards 1 and 2 (IAS1 & IAS2). The IA factors are summarised in Table 2.2 after being identified and analysed by the concept, and factors that have similarities in concept were removed to avoid duplication.

Table 2.2 Summary of IA factors from literature

Factors	Bunker	Cherdantseva & Hilton	MICT	CCEB	CESG	Chris Cope
Access Control	√		√			
Architecture and Planning	√					
Best practices		√				
Biometrics		√				
Business Alignment	√					√
Business Continuity Management	√	√	√			√
Certification and Accreditation		√		√		
Change Management			√			
Communication Security			√	√		
Compliance		√			√	
Computer Security				√		
Configuration and Patch Management	√					
Consider the Full Lifecycle					√	√
Cryptography	√	√	√	√		
Culture		√				
Data Protection	√					
Delivery Management	√					
Documentation		√	√			
Ethics		√				
Firewall		√				
Gateway Security			√			
Good Communication						√
Good Governance	√	√	√		√	√
Holistic Approach	√					√
Human Resource	√					
Identity Management	√					
Information Exchange/Sharing	√		√		√	
Law		√				
Leadership					√	
Logging, Auditing & Security Monitoring	√	√	√			
Motivation		√				
Network Security			√	√		
Organisation and Roles	√					
Physical Security	√	√	√	√		
Procedures		√				
Risk Management			√	√	√	√
Security Strategy	√	√	√	√		
Training, Education & Awareness	√	√	√		√	
Virtualization			√			

2.8 Challenges

Expensive and uneven infrastructures become an obstacle to the implementation of eGovernment in the local government; it also resulted in limited access to eGovernment in certain places (Hardjaloka, 2014). The Indonesian government does not have an interconnected government network and does not have a secure government network (Anggono, 2015). Moreover, at the local level, the available bandwidth is around 128 kbps to 1 Mbps, and the central level bandwidth is around 10 to 200Mbps, while the citizen-facing bandwidth is around 100 Mbps to 1 Gbps (Anggono, 2015). The length of optical fibre that is available is around 50,000 km. The Indonesian government owns about 300 data centres that are not yet integrated with each other and are without backup or a disaster recovery plan (Anggono, 2015).

Besides infrastructure, in implementing the eGovernment initiatives, cultural issues play a key role as these also influence any organisational changes regarding initiatives (Avgerou, 1993; Walsham, 1988). Culture is defined as values, beliefs, norms, and behavioural patterns of a group (Leung et al., 2005) that dictate how people think, solve problems, make decisions, and behave (Hall, 1976). In Indonesia, some cultural issues influence the process of eGovernment implementation, such as the following (Wicaksono, 2003; Djumadal, 2008; Hardjaloka, 2014):

- No culture of sharing,
- No culture of documenting,
- No full support from leaders,
- Resistance toward openness, and
- Resistance to change of mind-set.

In addition to infrastructure and cultural factors that hinder the implementation of eGovernment, according to Khalil, Lanvin & Chaudhry (2002), in developing countries such as Indonesia, the digital divide factor and trust and privacy must also be considered in the implementation of eGovernment. Differences in age, gender, income, education in Indonesia, have resulted in the emergence of the gap in access to technology (Yanti & Alamsyah, 2014; Puspitasari & Ishii, 2016; Sujarwoto & Tampubolon, 2016). In addition, to achieve the successful implementation of eGovernment, trust must be established between government institutions as well with the citizens.

Moreover, from the IA aspects, with the enormous amount of user information that must be managed, regarding the issue of privacy of information, the government should consider the responsibility with the intention that the user information is well protected (Khalil, Lanvin & Chaudhry, 2002). Data privacy laws and regulations do not exist in Indonesia, moreover, Indonesia

has no singular and unified act for privacy and data protection. (Palupy, 2011; Norton Rose Fulbright, 2014).

Furthermore, awareness, government systems, and capacity building are important in managing security within the organisation (Ardiyanti, 2014). The technical and procedural measures also need to be considered so that personnel in the organisation understand their role and the procedure in participating to actualise the security (Setiadi, Sucahyo & Hasibuan, 2012). The lack of experts in the field of security opens opportunities for cooperation with the private sector and international institutions (Setiadi, Sucahyo & Hasibuan, 2012; Operanata, 2015).

Other challenges regarding security in Indonesia are organisational structure and coordination. The creation of an organisation like a National Cyber Agency to be in control of handling information security issues is required to oversee the other organisations that already exist in managing government information security issues including eGovernment (Ardiyanti, 2014). With many government institutions in Indonesia, there is a need for coordination between institutions so that the duties of each institution do not overlap in assuring eGovernment services (Operanata, 2015; Ardiyanti, 2014).

From identifying these issues, it appears that many factors are challenging in the implementation of eGovernment services as well as IA. These factors need to be addressed in the proposed framework to ensure continuity of eGovernment services in Indonesia. All factors from challenges of eGovernment implementation and IA aspects after being analysed by concept and duplications removal are summarised in Table 2.3.

Table 2.3 Summary of factors from challenges

Factors	Khalil	Wicaksono	Djumadal	Palupy	Setiadi	Ardiyanti	Hardjaloka	Norton	Yanti	Anggono	Operananta	Puspitasari	Sujarwoto
Capacity Building					√	√							
Coordination											√		
Digital Divide	√						√		√			√	√
Infrastructure		√					√			√			
Integration					√	√							
International Cooperation					√	√							
Lack of Human Resources		√											
Leadership and Commitment			√							√			
Legal Aspect			√		√	√	√						
Limited Access		√					√						
No Culture of Documenting		√					√						
No Culture of Sharing		√	√				√						
Organisational Structures					√	√					√		
Resistant to Change			√										
Resistant to Openess			√										
Technical and Procedural					√	√							
Trust & Privacy	√			√				√					

2.9 Review of existing frameworks

The study of IA framework for eGovernment with the context in Indonesia so far has not existed, and so far, there have been only a few studies on IA for eGovernment. Considering InfoSec is still a part of IA and the issue of security cannot be separated from the implementation of eGovernment, therefore, besides discussing existing IA frameworks, this section also discusses existing InfoSec frameworks and model within Indonesian context or developing countries. There have been several studies identifying IA and security issues in eGovernment implementation.

Lambrinoudakis et al. (2003) developed a security policy model based on the public key infrastructure (PKI). This study focused on the security mechanisms of eGovernment information systems, which related to the hardware/software infrastructure of eGovernment. However, this study does not identify the human and management aspects in the model.

Alfawaz et al. (2007) focused on identifying the differences in eGovernment security between developing and developed countries. There is an indication that differences exist. Although the technology tends to be the same, the differences in environmental factors may affect the success or failure of eGovernment implementation. A framework is proposed as a result of an investigation involving a multi-methodological approach to defining fundamental differences that may occur between developed and developing countries. Of the factors identified in this study, there is no mention of the risk and incident handling aspect as well as the business continuity for eGovernment.

Wang and Sun (2009), proposed a framework of information security assurance system of eGovernment. The study analysed information security risks of eGovernment from three aspects: management, technology and laws. They suggested an integrated approach by identifying three key factors that are strategy, management and technology. These three factors cooperate closely with each other, form six major abilities: pre-warning, protection, examination, reacting, recovery and counterattack. However, this framework does not identify cultural and infrastructure factors.

Karokola et al. (2011) proposed a framework that integrates IT security services into eGovernment maturity models. This framework addressed both technical and non-technical factors that are necessary for eGovernment services and then integrated into the maturity model which consists five stages that are web-presence, interaction, transaction, transformation, continuous improvement. However, this study does not mention any of cultural or infrastructure factors.

Upadhyaya et al. (2012) developed an eGovernment security framework with a case study in Nepal. The proposed framework is a cost-effective security framework for developing countries. Factors

identified in the framework are management, awareness, training, and infrastructure. However, this framework does not identify risk management nor deal with business continuity in the event of an incident.

Setiadi, Sucahyo & Hasibuan (2013) introduced a security framework to secure eGovernment systems and processes. The framework combines both technical and non-technical aspects as a solution for eGovernment security. However, despite identifying these two aspects, the framework does not mention risk factors and business continuity in the event of system incidents.

Priyambodo and Prayudi (2015) proposed an information security strategy for mobile-based eGovernment systems. This strategy covers the aspects of data, service, human, policy, infrastructure, and technology. However, this strategy does not mention risk management and the handling of incidents to maintain business continuity. Table 2.4 provides a summary of the reviewed related works.

Table 2.4 Summary of reviewed existing eGovernment IA and InfoSec frameworks

Study	Types of Contribution	Indonesian Context	Evaluation
Lambrinoukadis et al. (2003)	Security policy model	No	The authors have developed a security policy model based on the public key infrastructure (PKI). However, this study does not identify the human and management aspects in the model.
Alfawaz et al. (2007)	Framework	No	This study was focused on identifying the differences in eGovernment security between developing and developed countries. Nevertheless, risk and incident handling and business continuity for eGovernment was not mentioned.
Wang and Sun (2009)	Framework	No	This study analysed information security risks of eGovernment from three aspects: management, technology and laws. However, this framework does not identify cultural and infrastructure factors.
Karokola et al. (2011)	Framework	No	The authors proposed a framework that integrates IT security services into eGovernment maturity models. However, there is no mention of cultural or infrastructure factors.
Upadhyaya et al. (2012)	Framework	No	The authors developed an eGovernment security framework with a case study in Nepal. However, risk management and business continuity in the event of an incident were not identified or discussed.
Setiadi, Sucahyo and Hasibuan (2013)	Framework	No	The authors introduced a security framework to secure eGovernment systems and processes. However, risk

			factors and business continuity in the event of system incidents were not considered.
Priyambodo and Prayudi (2015)	Security Strategy	Yes	The authors proposed an information security strategy for mobile-based eGovernment systems. Nonetheless, risk management and handling incidents to maintain business continuity were not considered.

2.10 Research gap

Indonesia is one of the developing countries and the largest country in the South East Asia region. The government recognised that information and communication technology (ICT) is facilitating the flow of information between governments and the public (Kominfo, 2015). Moreover, a developing country needs to emphasise optimising the use of IT investments and practices to develop the whole country (Abu-Musa, 2007). One way to optimise the use of IT investments is by implementing eGovernment that can improve the quality of government services that benefits society and business. In addition, eGovernment offers many solutions for organisations in developing countries, especially those countries aiming to become advanced (Khalil, Lanvin & Chaudhry, 2002).

In Indonesia, the implementation of eGovernment is still unsatisfying. Therefore, in order to support eGovernment implementation, it is essential to implement information assurance (IA). This is intended to reduce the risks to businesses in regard to information and information systems and ensuring the business continuity when incidents occur. Additionally, it is necessary to understand the practices and cultures which exist in the government agencies which are implementing IA. According to Rugman and Collinson (2006), nationality and culture tend to coexist, in addition, cultures vary between nations and these variations contribute to actual and significant differences in the ways that companies operate and people work. Moreover, employees' attributes and behaviours are affected by the culture in the organisation (Smircich, 1983). Further, managing Indonesian employees is not the same as leading Westerners, as Indonesia, like some Asian countries, is distinguished by high Power Distance and Collectivism (Irawanto, 2016). These characteristics are based on the Hofstede's cultural dimensions theory, which means people in organisations in Indonesia accepts an unequal, hierarchical distribution of power and people are supposed to be loyal to the group to which they belong (Hofstede, 2001). This cultural condition is stable and resistant to change as the people of any particular nationality are adjusted by certain patterns of socialization, education, and life experience (Hofstede, 2001). Therefore, it is

fundamental to understand cultures since it has impact on the effectiveness of managerial practices that can affect the implementation of IA in Indonesia.

Furthermore, studies carried out by Priyambodo and Prayudi in 2015 is one of the few information security for eGovernment studies that have been conducted in Indonesia, clearly indicating there are not enough studies in Indonesia. In addition, most studies have focused specifically on information security for eGovernment (e.g. Alfawaz et al., 2007; Wang and Sun, 2009; Karokola et al., 2011; Upadhyaya et al., 2012; Setiadi, Sucahyo and Hasibuan, 2013), and it is difficult to find studies in IA for eGovernment in Indonesia. Therefore, based on an intensive search, there is no specific study of IA for eGovernment within the Indonesian context. Thus, it can be said that this study is one of the preliminary studies in this field, and it will enrich the studies targeting factors of IA implementation for eGovernment in Indonesia in particular and in developing countries in general.

Therefore, a study on the implementation of IA for eGovernment in the Indonesian context is necessary. After reviewing previous studies, to the best of author's knowledge, there has not been a study that discusses IA for eGovernment for the Indonesian context. This study intends to fill the gap in the existing literature. The significance of this research lies in the success of examining what factors are associated with achieving IA for eGovernment in the Indonesian context as well as confirming those factors.

2.11 Research aims and objectives

The main study's objective is to investigate and identify the factors that encourage the successful implementation of IA for eGovernment in Indonesia. In addition, the study is designed to discuss some of the existing barriers to successful implementation, as well as providing help for some of the existing gaps in the literature. The study developed a framework by which one can successfully analyse the current IA for eGovernment situation, as well as providing insights into the future role of government in improving IA performance. Furthermore, the other aims are:

1. Identifying the obstacles and success factors of IA in general.
2. Identifying the status of IA and eGovernment in Indonesia.
3. Finding the factors that encourage successful implementation of IA for eGovernment in Indonesia.
4. Developing a validated IA framework.
5. Conducting case studies on government organizations in Indonesia to measure their IA implementation's success.

6. Developing a validated instrument, able to measure the success of IA implementation for eGovernment in public organisations in Indonesia.

2.12 Research question

This research will study these factors and propose a framework within the Indonesian context that can be used as guidance in achieving IA for eGovernment. There is a research question that should also be answered:

Q1. What form of IA framework is appropriate for the Indonesian eGovernment?

This question is divided into two sub-questions:

- Q1.1 What are the issues and challenges facing the implementation of IA for eGovernment in Indonesia?
- Q1.2 How can the proposed framework be evaluated to efficiently and appropriately meet the demands in assuring eGovernment services within the Indonesian context?

Q2. How can the IA implementation process for eGovernment within the Indonesian context be measured?

Q3. Is the developed measuring instrument an appropriate instrument to measure the implementation process of IA for eGovernment in government organisations in Indonesia?

2.13 Summary

This chapter presented the discussion of the concept of eGovernment and IA and has also mentioned the relationship of IA with InfoSec and the importance of IA for organisations as well as eGovernment. To achieve the success of IA in eGovernment, the implementation must focus on a range of factors. Factors required in the implementation of IA for eGovernment in the Indonesian context were discussed in this chapter. These factors were extracted from international IA standards and IA CSFs. In addition, this chapter also addressed the challenges of IA implementation for eGovernment in the context of Indonesia.

Chapter 3 **Proposed Framework**

In the previous chapter, the factors that need to be considered in applying IA for eGovernment services were discussed. These factors are generally universal, but there are also factors that are more specific for developing countries such as Indonesia. Until now, there has been no research on IA for eGovernment in Indonesia. In this chapter, the proposed framework of IA for eGovernment in Indonesia is presented.

3.1 Construction of the framework

A framework is a basic conceptional structure (visual or written) with items to be studied -the key factors, concepts, or variables- and the presumed relationships among them (Miles & Huberman, 1994). In this study, a framework defined as a concept with list of identified factors that can be expanded into something useful. The purpose of the construction of the framework in this research is to identify the factors to implement IA in eGovernment in Indonesia. The development of this framework is divided into four stages. Figure 3.1 illustrates the framework construction stages.

Figure 3.1 Framework construction stages

The first stage is identifying the factors for the implementation of IA from existing IA frameworks that have been recognised and have become international best practices for organisations. After removing the duplication factors, 23 factors of IA from ISO/IEC 27001, IASME, and COBIT 5 for Assurance, which are summarised in Table 2.1, were used in the development of this framework. These factors are necessary for providing requirements for establishing, implementing, maintaining, and continually improving IA.

The second phase is determining success factors in the implementation of IA in addition to the international standard factors. At this stage, after duplication factors were removed, 39 the factors were identified from reviewing international research publications on success factors of IA and summarised in Table 2.2.

The third stage is identifying the challenges that affect the process of implementation of IA for eGovernment in Indonesia. The 17 factors that are summarised in Table 2.3, after duplication factors were removed, were identified by reviewing scientific publications concerning the challenges of eGovernment implementation in developing countries including Indonesia.

The fourth and last stage is evaluating all 79 factors that have been identified in the previous stages. The identified factors were harmonised to form a connected whole and synthesised into new factors. The author made all the decisions during the harmonisation process. All the decisions for the harmonisation process were made after considering each factor by its concept and scope. This is an important contribution of this work, as it establishes a framework for IA, based on internationally recognised standards of IA, IA literature, and Challenges. Figure 3.2 clarifies Phase 1 of the Stage 4 process.

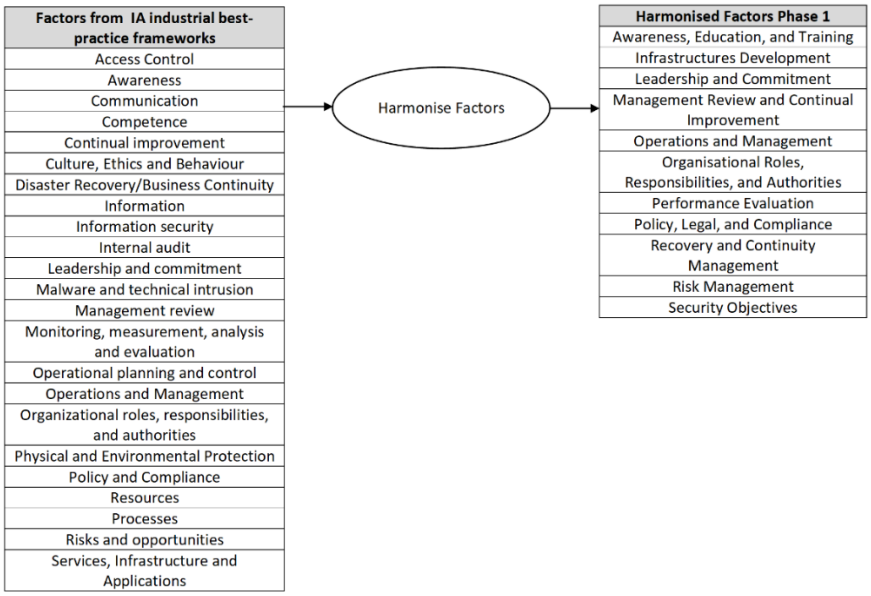

Figure 3.2 Phase 1 of forming the IA framework

After removing the duplication factors, the remaining factors were harmonised by concept and scope. Which means, every factor is analysed by its purpose, description, meaning, and then synthesised into new factors. For example, Access Control, Information security, Malware and technical intrusion, Physical and Environmental Protection all have a same scope. By definition, these factors have similar purposes that is still within the scope of the security aspect. Therefore, these factors were synthesised into a new factor namely Security Objectives. The new factor name came from the purpose of the factor that is to deal with security aspect during implementation of IA which covers physical, access and information security.

Furthermore, all the factors resulting from harmonisation process and influenced by harmonised factors are Awareness, Education, and Training, Leadership and Commitment, Management Review and Continual Improvement, Infrastructures Development, Operations and Management, Organisational Roles, Responsibilities, and Authorities, Performance Evaluation, Policy, Legal, and Compliance, Recovery and Continuity Management, Risk Management, Security Objectives. Table 3.1 presents factors from the results of the harmonisation process Phase 1.

Table 3.1 Factors from the phase 1 of harmonisation

Factor name	Source
Awareness, Education, and Training	Awareness
	Competence
	Culture, Ethics and Behaviour
Leadership and Commitment	Communication
	Leadership and commitment
Management Review and Continual Improvement	Continual improvement
	Management review
Infrastructures Development	Services, Infrastructure and Applications
Operations and Management	Operational planning and control
	Operations and Management
	Processes
Organisational Roles, Responsibilities, and Authorities	Organisational roles, responsibilities and authorities
Performance Evaluation	Internal audit
	Monitoring, measurement, analysis and evaluation
Policy, Legal, and Compliance	Policy and Compliance
Recovery and Continuity Management	Disaster Recovery/Business Continuity
Risk Management	Information
	Resources
	Risks and opportunities
Security Objectives	Access Control
	Information security
	Malware and technical intrusion
	Physical and Environmental Protection

Although these factors are from international standards, it is still necessary to identify other factors from relevant literature that are expected to complement IA aspects that are not covered by the standards. Figure 3.3 illustrates the Phase 2 of the harmonisation integrating IA factors from the literature into the factor from Phase 1.

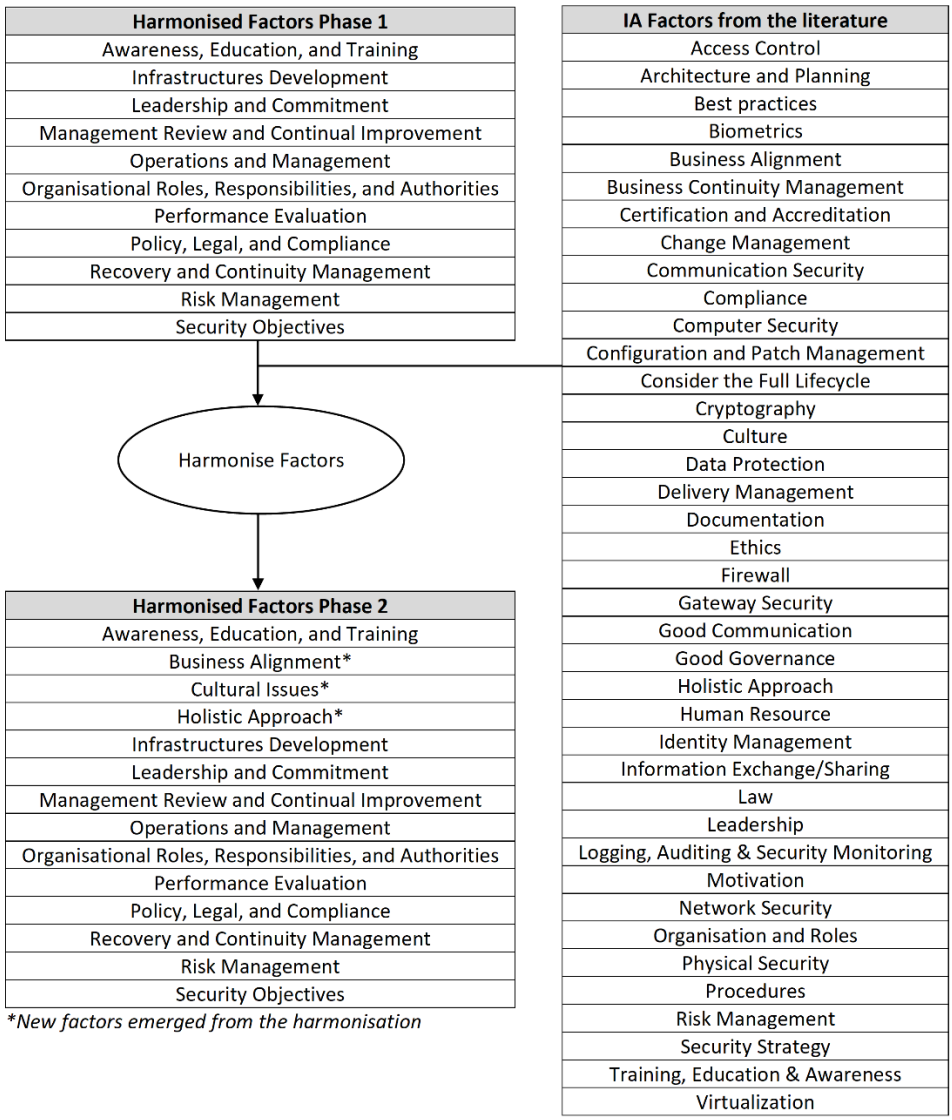

Figure 3.3 Phase 2 of forming the IA framework

New factors emerged from the Phase 2 of harmonisation process and influenced by the Phase 1 harmonised factors are Business Alignment, Cultural Issues, and Holistic Approach. Table 3.2 presents factors from the results of the harmonisation process Phase 2.

Table 3.2 Factors from the phase 2 of harmonisation

Factor name	Source
Awareness, Education, and Training	Ethics
	Training, Education & Awareness
Business Alignment	Business Alignment
Cultural Issues	Culture
	Motivation
Holistic Approach	Holistic Approach
Leadership and Commitment	Good Communication
	Leadership
Operations and Management	Architecture and Planning
	Change Management
	Configuration and Patch Management
	Delivery Management
	Good Governance
	Procedures
	Virtualization
Organisational Roles, Responsibilities, and Authorities	Human Resource
	Organisation and Roles
Performance Evaluation	Consider the Full Lifecycle
Policy, Legal, and Compliance	Best practices
	Certification and Accreditation
	Compliance
	Documentation
	Law
Recovery and Continuity Management	Business Continuity Management
Risk Management	Risk Management
Security Objectives	Access Control
	Biometrics
	Communication Security
	Computer Security
	Cryptography
	Data Protection
	Firewall
	Gateway Security
	Identity Management
	Information Exchange/Sharing
	Logging, Auditing & Security Monitoring
	Network Security
	Physical Security
	Security Strategy

Moreover, it is still necessary to identify other factors from relevant literature on challenges for the IA and eGovernment implementation in Indonesia to complement the identified factors. Figure 3.4 clarifies the Final Phase of the harmonisation process to integrate the factors from challenges literature into the harmonised factors from Phase 2.

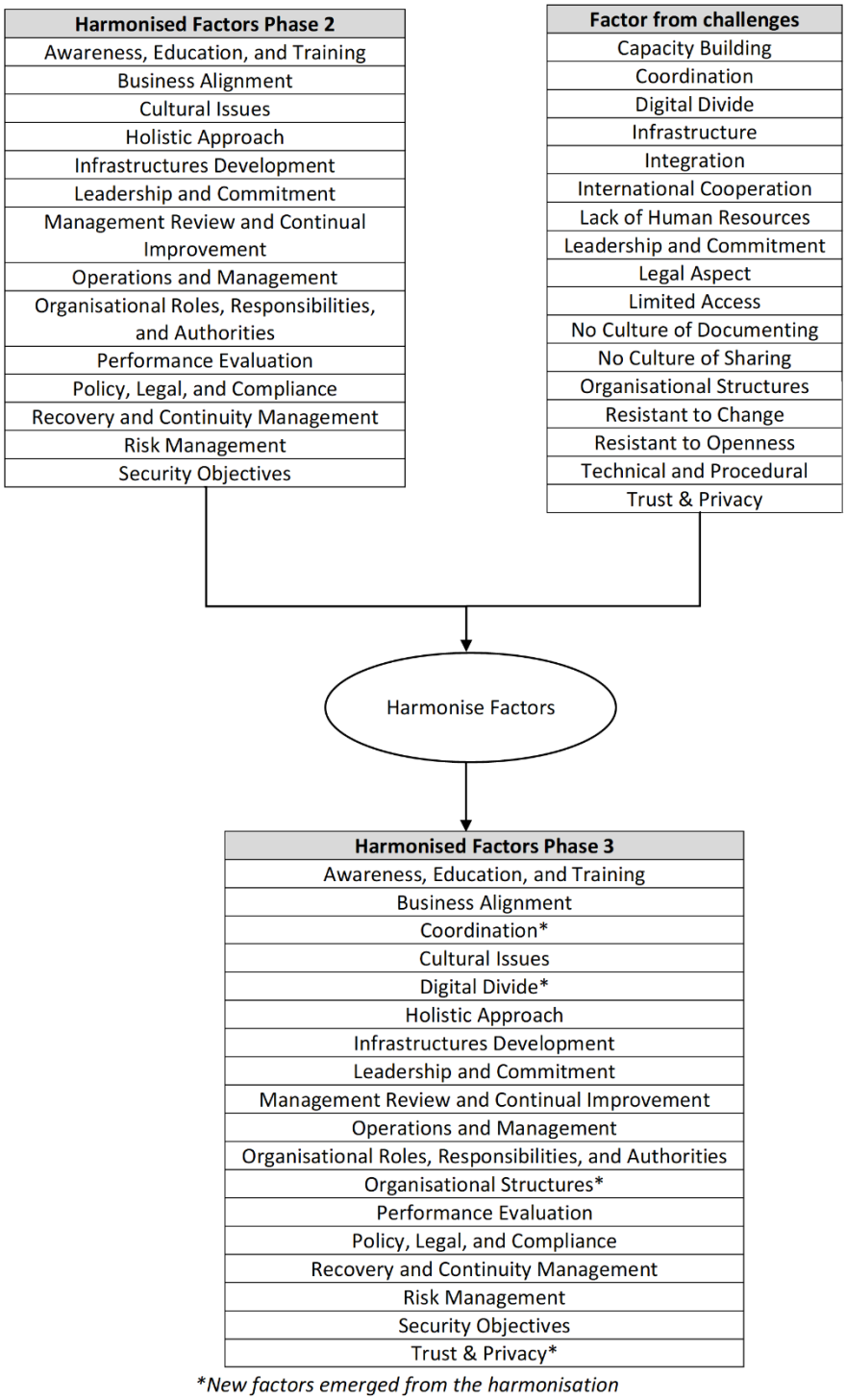

Figure 3.4 Final phase of forming the IA framework

The new factors resulting from synthesising process and influenced by factors that have been harmonised by scope and concept in phase 2 are Coordination, Digital Divide, Organisational Structures, and Trust & Privacy. Table 3.3 presents factors from the results of the harmonisation process Phase 3.

Table 3.3 Factors from the final phase of harmonisation

Factor name	Source
Awareness, Education, and Training	Capacity Building
	Lack of Human Resources
Coordination	Coordination
	Integration
Cultural Issues	Legal Aspect
	No Culture of Documenting
	No Culture of Sharing
	Resistant to Change
	Resistant to Openness
Digital Divide	Digital Divide
Infrastructure Development	Infrastructure
	Limited Access
Leadership and Commitment	Leadership and Commitment
Operations and Management	Technical and Procedural
Organisational Structures	International Cooperation
	Organisational Structures
Trust and Privacy	Trust & Privacy

Furthermore, all 18 factors from the harmonisation process are presented in Table 3.4. The Table demonstrates the gaps between IA industrial best-practice frameworks, IA literature, and challenges literature. It also shows how these works of literature complement each other in constructing the IA framework.

Table 3.4 IA factors from the harmonisation process

Factors	IA standard-based frameworks	IA literature	Challenges
Leadership and Commitment	√	√	√
Policy, Legal, and Compliance	√	√	
Management Review and Continual Improvement	√		
Holistic Approach		√	
Business Alignment		√	
Organisational Roles, Responsibilities, and Authorities	√	√	
Awareness, Education, and Training	√	√	√
Risk Management	√	√	
Security Objectives	√	√	
Operations and Management	√	√	√
Performance Evaluation	√	√	
Recovery and Continuity Management	√	√	
Cultural Issues		√	√
Infrastructures Development	√		√
Digital Divide			√
Trust and Privacy			√
Organisational Structures			√
Coordination			√

Moreover, the identified factors are then categorised based on the scope and association. The three categories formed from the process are organisational management, implementation management, and Indonesian context. Factors that are closely related to managerial and human aspects are incorporated into the organisational management category. Further, more technical factors are categorised as implementation management. Finally, context-focused Indonesian factors are then incorporated into the Indonesian context. Table 3.5 presents the factors that have been categorised into three categories.

Table 3.5 Mapping the IA factors with the categories

Categories	Factors
Organisational Management	Leadership and Commitment
	Policy, Legal, and Compliance
	Management Review and Continual Improvement
	Holistic Approach
	Business Alignment
	Organisational Roles, Responsibilities, and Authorities
	Awareness, Education, and Training
Implementation Management	Risk Management
	Security Objectives
	Operations and Management
	Performance Evaluation
	Recovery and Continuity Management
Indonesian Context	Cultural Issues
	Infrastructures Development
	Digital Divide
	Trust and Privacy
	Organisational Structures
	Coordination

3.2 Proposed Framework

The framework consists of 18 factors that are divided into three categories: organisational management, implementation management, and Indonesian context. The proposed framework is shown in Figure 3.5 and described in the following section.

Figure 3.5 IA framework for eGovernment in the Indonesian context

Table 3.6 displays the framework categories includes the factors that have been identified along with the sources of the literature. In the next section, each factor will be further explained.

Table 3.6 IA framework for eGovernment in the Indonesian context

Categories	Factors	Sources
Organisational Management	Leadership and Commitment	(Djumadal, 2008; Bunker, 2012; Cherdantseva & Hilton, 2013; ISACA, 2013; ISO/IEC 27001, 2013; MICT, 2014; Anggono, 2015; Cope, 2015)
	Policy, Legal, and Compliance	(IASME, 2013; Cherdantseva & Hilton, 2013; ISACA, 2013; ISO/IEC 27001, 2013; MICT, 2014; CESG, 2015)
	Management Review and Continual Improvement	(ISO/IEC 27001, 2013)
	Holistic Approach	(Bunker, 2012; Cope, 2015)
	Business Alignment	(Bunker, 2012; Cope, 2015)
	Organisational Roles, Responsibilities, and Authorities	(Bunker, 2012; IASME, 2013; ISACA, 2013; ISO/IEC 27001, 2013)
	Awareness, Education, and Training	(Wicaksono, 2003; Bunker, 2012; Setiadi, Sucahyo & Hasibuan, 2012; IASME, 2013; Cherdantseva & Hilton, 2013; ISACA, 2013; ISO/IEC 27001, 2013; Ardiyanti, 2014; MICT, 2014; CCEB, 2015; CESG, 2015)
Implementation Management	Risk Management	(IASME, 2013; ISACA, 2013; ISO/IEC 27001, 2013; MICT, 2014; CCEB, 2015; CESG, 2015; Cope, 2015)
	Security Objectives	(Bunker, 2012; IASME, 2013; Cherdantseva & Hilton, 2013; ISO/IEC 27001, 2013; MICT, 2014; CCEB, 2015; CESG, 2015)

	Operations and Management	(Bunker, 2012; Setiadi, Sucahyo & Hasibuan, 2012; IASME, 2013; Cherdantseva & Hilton, 2013; ISACA, 2013; ISO/IEC 27001, 2013; Ardiyanti, 2014; MICT, 2014; CESG, 2015; Cope, 2015)
	Performance Evaluation	(Bunker, 2012; Cherdantseva & Hilton, 2013; IASME, 2013; ISACA, 2013; ISO/IEC 27001, 2013; MICT, 2014)
	Recovery and Continuity Management	(Bunker, 2012; IASME, 2013; Cherdantseva & Hilton, 2013; ISO/IEC 27001, 2013; MICT, 2014; Cope, 2015)
Indonesian Context	Cultural Issues	(Wicaksono, 2003; Djumadal, 2008; Setiadi, Sucahyo & Hasibuan, 2012; Cherdantseva & Hilton, 2013; Ardiyanti, 2014; Hardjaloka, 2014)
	Infrastructures Development	(Wicaksono, 2003; ISACA, 2013; Hardjaloka, 2014; Anggono, 2015)
	Digital Divide	(Khalil, Lanvin & Chaudhry, 2002; Hardjaloka, 2014; Yanti & Alamsyah, 2014; Puspitasari & Ishii, 2016; Sujarwoto & Tampubolon, 2016)
	Trust and Privacy	(Khalil, Lanvin & Chaudhry, 2002; Palupy, 2011; Norton Rose Fullbright, 2014)
	Organisational Structures	(Setiadi, Sucahyo & Hasibuan, 2012; Ardiyanti, 2014; Operananta, 2015)
	Coordination	(Setiadi, Sucahyo & Hasibuan, 2012; Ardiyanti, 2014; Operananta, 2015)

3.2.1 Organisational management

The following factors are associated with organisational management in implementing IA for eGovernment within the Indonesian context.

1. Leadership and Commitment

   Leadership and commitment from the top of the organisation in the implementation of IA are critical for the achievement of IA through the initial planning. Top management must ensure that the policy and objectives of IA are in line with business needs. In addition, the availability of required resources should be ensured.

2. Policy, Legal, and Compliance

   The policy aims to guide the IA to be in line with business needs. The legal department needs to ensure legal certainty for the use of information, intellectual property rights, and the use of software and other products. Furthermore, the compliance of the information systems with policies and standards also need to be ensured.

3. Management Review and Continual Improvement

   Top management should undertake periodic review of the continuing suitability, adequacy, and effectiveness of the IA. From the reviews, continual improvement for the suitability, adequacy, and effectiveness of the IA is expected.

4. Holistic Approach

   The IA shall be treated as a unity of the physical, procedural, personnel, and technical security. Moreover, IA is not just a matter of technology, as most threats come from humans. By treating IA holistically, defences are layered in-depth and the weakness in one aspect can be covered in other aspects.

5. Business Alignment

   In practice, IT and security do not work independently, but both support the business. The IA should be able to accommodate business needs. Since business runs on risk, by planning IA that focuses on business objectives, business risk can be minimised, and information held by an organisation is assured.

6. Organisational Roles, Responsibilities, and Authorities

   Top management must ensure roles in the organisation. Ensuring responsibility and authority by top management is required to confirm IA is in accordance with the standard. Top management should also receive reports related to IA performance.

7. Awareness, Education, and Training

   People who work in the organisation must be aware of the information policy and its contribution to the effectiveness and performance of the IA as well as the implications of not complying with the IA requirements. Moreover, all employees working in the organisation are required to undergo relevant training and education corresponding to their job functions. It is intended that all staff will be competent in their respective fields.

3.2.2 Implementation management

The following factors are associated with implementation management in implementing IA for eGovernment within the Indonesian context.

1. Risk Management

   The first step in risk management is asset enumerating and planning, which aims to calculate assets owned by the organisation and categorise them. In addition, this process also plans the use of assets for the organisation. Assets that have been identified will be assessed to define the total risk of the information asset. From the results of the

assessment, the treatments for risks will be determined. Risks cannot always be eliminated but can be minimised.

2. Security Objectives

   Information security objectives must be determined relevant to the functions and levels and be consistent with the information security policy. Moreover, in determining the security objectives, the needs of information security, as well as the results of the risk assessment and risk treatment, must be considered.

3. Operations and Management

   Organisations must ensure the plan, implementation, and control needed to comply with information security requirements. To ensure optimal security, it is necessary to update the security systems in accordance with the latest updates from the provider.

4. Performance Evaluation

   Performance evaluation includes internal audits, monitoring, measurement, analysis, and evaluation. Internal auditing needs to be done to confirm whether the IA complies with the needs of the organisation and the international standards. Information relating to the effectiveness of implementation and maintenance of IA will also be obtained from the results of the audit. Monitoring, measurement, analysis, and evaluation are used to evaluate the performance and effectiveness of the IA.

5. Recovery and Continuity Management

   Backup and restore is the capability to maintain the integrity and availability of information systems during an incident or disaster. In the event of major failures of information systems, business continuity must be maintained and work as usual.

3.2.3 Indonesian context

The challenges related to factors in the context of implementing eGovernment and IA in Indonesia as well as other developing countries are presented in the following section.

1. Cultural Issues

   Cultural issues need to be considered in the implementation of IA. This is related to cultural issues that influence behaviour in organisations in Indonesia that can affect IA performance.

2. Infrastructure Development

   Implementation of eGovernment requires good infrastructures for the system to able to provide services as intended. In addition, infrastructures are also needed for the

information security process to be achieved according to the security objectives. Indonesia and other developing countries generally have difficulty in developing basic infrastructures.

3. Digital Divide

   Differences in class, race, ethnicity, and geography in developing countries, especially Indonesia, have resulted in the emergence of the gap in access to technology, especially the Internet. This issue should be addressed regarding IA performance, especially as under-developed regions still need to achieve the initial objectives.

4. Trust and Privacy

   To achieve the successful implementation of eGovernment, trust must be established between government institutions as well with the citizens. With the enormous amount of user information that must be managed, regarding the issue of privacy of information, the government should consider the responsibility with the intention that the user information is well protected.

5. Organisational Structures

   The creation of an organisation like a National Cyber Agency to be in control of handling information security issues is required. This organisation will oversee the other organisations that already exist in managing government information security issues including eGovernment.

6. Coordination

   With many government institutions in Indonesia, there must be coordination between institutions so that the duties of each institution do not overlap in protecting eGovernment information.

3.3 Summary

This chapter has presented a description of all phases of the development as well as the proposal for an IA framework for eGovernment in Indonesia. The development of the framework was divided into four stages. The first stage was identifying the IA factors from international best practices. The second stage was determining IA success factors from the literature, and the third stage was identifying the challenges. In the fourth stage, all 79 factors were analysed and harmonised by their concepts and then synthesised into new factors. The remaining 18 factors were divided into three categories based on the scope and association. The next chapter is the research methodology for this research.

Chapter 4 **Research methodology**

This chapter presents the methodology used to review and confirm the IA framework for eGovernment in Indonesia that has been proposed in the previous chapter. This chapter also presents the methodology that will be carried out for future work. In the following sections, the research methodologies for this study are being discussed. The triangulation method is considered which will use the quantitative and the qualitative methods for the data collection process. Moreover, the statistical techniques, Bonferroni Correction and One Sample T-Test will used to analyse the data as well as Cronbach's Alpha will be used to measure the reliability. Further, Goals Question Metric method is chosen to develop the instrument. In addition, a discussion of the research methodology designed for this research is also presented.

4.1 Research methods

Research methods are the techniques used to conduct research such as collecting and analysing data (Kothari, 2004). The qualitative, quantitative, and mixed methods are the three main methods widely used in the area of IS research (Recker, 2013). Following subsections present a brief description of each method.

4.1.1 Qualitative method

The qualitative method aims at describing and analysing phenomena to get new information and helps to discover new theoretical insights (Recker, 2013; Venkatesh & Brown, 2013). The qualitative approach is related to data in the form of ideas, perceptions, opinions, or beliefs that are not easily shown in the form of numbers. Data collection methods in qualitative approach include interviews, observations, focus groups, and document analysis (Anderson, 2010; Recker, 2013).

Interviews are the most commonly used method of data collection in qualitative research studying human phenomena (Carter et al., 2014). An interview can be described as a conversation between individuals with the purpose of opening up the possibility of gaining insight into a certain topic or subject (Schostak, 2006). There are three types of interviews that are frequently practised in qualitative research, namely structured, unstructured, and semi-structured interviews (Qu & Dumay, 2011). The structured interview key feature is that it requires immediate responses from a limited number of response categories to answer a series of pre-established questions (Qu & Dumay, 2011). On the other hand, unstructured interview allows freedom and flexibility to both interviewers and interviewees in terms of organising the interview content and questions (Edwards

& Holland, 2013). Lastly, the semi-structured interview is a more flexible version of structured interview which offers flexibility on the part of the interviewer to probe answers and ensure a dialogue (Edwards & Holland, 2013).

In determining participants, the qualitative approach using sampling techniques, which is the process of selecting a sample of a population for purposes of making observations (Bhattacherjee, 2012). Sampling techniques can be divided into two categories namely probability (random) sampling that the sampling results can be generalised; and the other is non-probability sampling, which results from the sampling cannot be generalised back to the population (Bhattacherjee, 2012). Participants often are chosen based on certain properties or expertise they possess (Recker, 2013). The size of sample depends on saturation being reached, the condition for this is when no new knowledge can be collected (Guest, Bunce & Johnson, 2006).

The identification and analysis of data from qualitative research are necessary in order to interpret the data. The most popular technique for analysing qualitative data is coding (Creswell, 2012; Recker, 2013). Coding means categorising the data by assigning labels or meaning related to the main theme or topic being examined in the study. The two steps of coding are generating meaningful data units and classifying and ordering the data units (Alshenqeeti, 2014).

4.1.2 Quantitative method

The quantitative method is frequently used to confirm previously developed hypotheses and it involves the collection, analysis, and interpretation of data that can be expressed in numbers (Recker, 2013; Venkatesh & Brown, 2013). A common way for data collection in a quantitative approach is by questionnaire (Recker, 2013). The main benefit of a questionnaire is that it can be used to collect data from a large number of respondents (Lazar & Preece, 2002). A questionnaire consists of a set of questions to gather responses from participants. To record the answers from respondents in a questionnaire, a Likert scale is commonly used (Saunders, Lewis & Thornhill, 2009). A Likert scale is a technique that can measure the attitudes that provide correlation between scores and case history (Likert, 1932).

The quantitative method depends on random sampling, where participants are selected randomly from a wider population (Recker, 2013). The sample size must be sufficient to be able to provide reliable results that can be generalised to the target population and it depends on the type of statistical test that will be conducted (Bhattacherjee, 2012). To determine this, the statistical power analysis programme, G* Power, can be used to calculate the minimum sample size (Faul et al., 2009). Moreover, there is also a central limit theorem that states, as the sample size increases, which is

usually defined as greater than 30, the sampling distribution will be normally distributed regardless of the shape of the population from which the sample was drawn (Field et al., 2013).

Data collected through a quantitative approach can be analysed in two different techniques, descriptive and inferential (Bhattacherjee, 2012). Descriptive analysis is a statistical technique that is used to describe, combine, and present the population or the dataset under study. Inferential analysis refers to statistical technique to test hypotheses. A software program such as SPSS can be used to analyse quantitative data (Recker, 2013).

One method to test the hypotheses is the t-test method, in which the t-test method is divided into three, one-sample t-test, paired sample t-test and independent sample t-test. The t-test can be used to determine whether there is a statistically significant difference in the mean of the sample taken. It can also be used to test if two group means are different (Field, 2009). In t-test, there are two error types that should be specified, which are alpha (α) and beta (β). Error type 1 is alpha that occurs when the true null hypothesis is rejected, while error type 2 is beta, which occurs when the null hypothesis is wrong but not rejected.

4.1.3 Mixed-methods

Mixed-methods is an approach that combines qualitative and quantitative methods in a single study (Tashakkori & Teddlie, 2010). The method incorporates the strengths of quantitative and qualitative methods and offers a greater understanding of a phenomenon that each of these methods individually cannot offer (Venkatesh et al., 2013).

There are five main purposes for conducting a mixed-methods approach (Johnson & Onwuegbuzie, 2004):

- Triangulation – refers to confirming findings from one study using different methods.
- Complementarity – refers to elaborating findings from one study using different methods.
- Initiation – refers to discovering contradictions that will lead to reframing the research questions.
- Development – refers to findings from one study to inform other methods.
- Expansion – refers to expanding the scope of the research using different methods to study different problems.

A triangulation method is an approach that combines two or more angles for investigating a problem, in order to cross-validate or confirm the findings from different sources (Jupp, 2006). The

method is aimed at increasing the robustness of findings (Recker, 2013). There are four different forms of triangulation (Jupp, 2006):

- Data triangulation – refers to collecting data from different sources.
- Investigator triangulation – refers to using different researchers to collect and analyse the data in order to mitigate the subjective influence of individuals.
- Theoretical triangulation – refers to approaching data from different theoretical perspectives.
- Methodological triangulation – refers to using different methods to collect, analyse, interpret the data in order to confirm the findings.

4.1.4 Bonferroni correction

Bonferroni correction is an adjustment made to P values when performing several dependent or independent statistical tests simultaneously on a single data set (Napierala, 2012). A Bonferroni correction should be considered when it is essential to avoid a type I error (Armstrong, 2014). Bonferroni correction can be performed by dividing alpha (α) by the number of items being used (Napierala, 2012).

4.1.5 Cronbach's alpha

Cronbach's alpha is a reliability test to measure the internal consistency of a test or scale (Tavakol & Dennick, 2011). Cronbach's alpha reliability test can help researchers to generate trustworthy results (Tavakol & Dennick, 2011). Cronbach's alpha is expressed as a number between 0 and 1, with ranges, if the reliability score is less than 0.6, it is considered poor, while around 0.6 is considered as moderate, good if around 0.7 and very good at 0.8 or above (Bryman & Cramer, 2001).

4.1.6 Goals question metric

Goals Question Metric (GQM) is a technique to identify meaningful metrics for the measurement process (Basili, Caldiera, & Rombach, 1994). It helps to determine the strengths and weaknesses of the current processes, and it provides a rationale for adopting/refining techniques, to evaluate the quality and impact of a specific process. GQM emphasizes the need to establish an explicit measurement goal, define a set of questions to achieve the goal, and identify metrics to answer the questions. The six-step GQM process includes, develop a set of goals, generate questions that define those goals, specify the measures needed to be collected. develop mechanisms for data

collection, collect, validate and analyze the data, analyse the data to assess conformance to the goals and to make recommendations for future improvements (Basili, Caldiera, & Rombach, 1994).

4.1.7 Case study

A case study is an empirical inquiry that investigates a contemporary phenomenon within its real-life context; especially when the boundaries between phenomenon and context are not clearly evident (Yin, 2003). Case studies are often used when there is a need for a detailed understanding in order to provide the researcher with rich data for a particular topic. A case study may be literally replicated, when the case is selected to predict similar results, or it is theoretically replicated, when the case is selected to predict contrasting results for predictable reasons (Yin, 2003).

4.2 Research design

In this study, the mixed-methods approach was selected to review and confirm the factors identified for IA framework for eGovernment in Indonesia. The reason to choose the mixed-methods is that this method can combine the qualitative and quantitative method and incorporates the strength of each method and therefore is able to increase the validity and test the hypotheses. The next section discusses the application of these methods in this study.

4.2.1 Triangulation

Methodological triangulation was selected and applied in this study. The reason to use the triangulation method is based on the purpose of this study, which is intended to examine and confirm the factors that have been identified for IA framework for eGovernment in Indonesia. The triangulation method is able to combine the qualitative method and the quantitative method. For this study, the qualitative method is useful in obtaining the differentiated opinions of the developed framework and exploring more issues and challenges facing the implementation of IA for eGovernment in Indonesia, which then will answer the research question Q1.1. Moreover, the quantitative method is useful to confirm the reviewed framework in order to ensure the framework will efficiently and appropriately meet the demands in assuring eGovernment services within the Indonesian context and thus will answer the research question Q1.2. Figure 4.1 illustrates the triangulation method for this study.

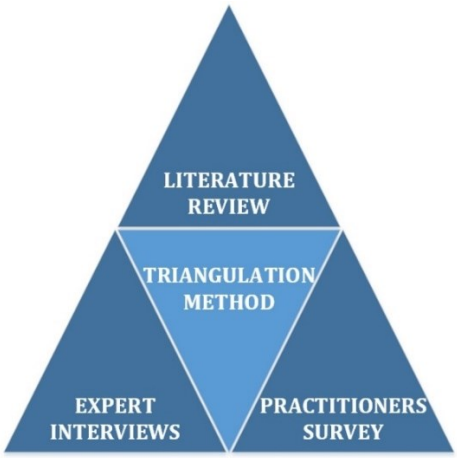

Figure 4.1 Triangulation method

The triangulation method consists of three phases. The first phase is the literature review, which is conducted to identify the framework factors. The second phase, using qualitative approach, is the expert interviews that aim to review the proposed framework. The final phase is a survey of practitioners using quantitative approach aimed at confirming the framework.

4.2.2 Expert interviews

Expert interviews were conducted to review the factors identified for the IA framework for eGovernment with the context in Indonesia. The interviews were in the form of qualitative interviews, which were aimed at reviewing the proposed IA framework. The proposed framework was reviewed by conducting interviews with IA experts, which also include information security experts and eGovernment experts in Indonesia who have at least five years of experience. Interviews were conducted face-to-face in Indonesia and recorded using a mobile phone application. Interview questions were semi-structured, which includes closed-ended and open-ended questions. Close-ended questions were intended to attain expert general information, while open-ended questions were intended to attain opinions on the factors that have been identified and additional information on factors other than those already identified.

4.2.2.1 Expert Interviews Design

The interviews were conducted with eight experts. To avoid sampling bias, all the experts selected for the interviews are from different organisations. The only characteristic they shared was the fact they have at least five years of experience in the field of IA, InfoSec or eGovernment. A procedural bias was also avoided by not giving a time limit for answering questions. Lastly, to avoid the participant bias, the experts were ensured that everything is confidential and their opinions were captured by asking open-ended questions which allow information to flow more freely.

The interviews were divided into two parts. The first part was designed for collecting general information. The second part was designed for finding out experts' opinion about factors affecting IA implementation for eGovernment in Indonesia. During the interviews, participants were given an opportunity to ask clarification questions immediately after they saw the framework; this process lasted between 5 and 10 minutes. Once this had been done, the participants were asked closed-ended questions. These closed-ended questions pertained to general demographic information. Then the experts were asked to provide their opinions on each factor. The interviews lasted about 30 to 60 minutes and a mobile phone was used to record the interviews, in case of the need to replay the interviews. Permission was obtained from all the interviewees before any recordings were made.

The full list of the interviews questions is provided in Table 4.1. The interview questions were developed by the author and then pre-tested on a few people before its official use. The interview questions need to be understandable and in the same way by all respondents. Therefore, in order to check how the interview questions perform for the effectiveness of the results, a pre-test was carried out with two experts who participated in the study to validate the clarity and organisation of interview questions. The alterations they recommended were not substantial and pertained to the editing of certain complicated sentences.

Table 4.1 Interview questions

Section A
Explanation: This section is used to collect your general information. Please consider all the options in each question carefully, and tick only one answer. 1. Which company or organisation do you work for? 2. Do you have any experience in the fields of Information Security, Information Assurance or eGovernment? □ Information Security □ Information Assurance □ eGovernment □ All of them □ Other _____ 3. How many years of experience do you have in the field you mentioned above?
Section B
1. The following discuss the organisational management factors that affect IA implementation for eGovernment in Indonesia. Please state whether you find each organisational management factor is important or not and why. • Leadership and Commitment • Policy, Legal, and Compliance • Management Review and Continual Improvement • Holistic Approach • Business Alignment

• Organisational Roles, Responsibilities, and Authorities • Awareness, Education, and Training
2. The following discuss the implementation management factors that affect IA implementation for eGovernment in Indonesia. Please state whether you find each implementation management factor is important or not and why. • Risk Management • Security Objectives • Operations and Management • Performance Evaluation • Recovery and Continuity Management
3. The following discuss the Indonesian context factors that affect IA implementation for eGovernment in Indonesia. Please state whether you find each Indonesian context factor is important or not and why. • Cultural Issues • Infrastructures Development • Digital Divide • Trust and Privacy • Organisational Structures • Coordination
4. Are there any factors missing? 5. Would you change any of these factors? 6. Can you tell me more about factors influence information assurance implementation for eGovernment in Indonesia?

4.2.2.2 Expert Interviews Sample Size

Qualitative research usually depends on non-probability sampling for deciding the sample size, by which respondents are selected in accordance with non-random criteria (Bhattacherjee, 2012). Expert sampling was chosen as the interviews were aimed to get opinions from experts. In expert sampling, participants are chosen based on knowledge or expertise they possess (Bhattacherjee, 2012). The size of the sample depends on saturation being reached, whereby there is no new knowledge can be collected (Guest, Bunce & Johnson, 2006). According to Romney et al. (1986), in qualitative interviews with respondents who have substantial knowledge and expertise in the topic of inquiry, the saturation can be achieved with around four to five respondents. Moreover, there is a Discounted Expert Review Theory according to which 75% of the usability can be found between three and five experts, after which it reaches a point of saturation (Rogers et al, 2011). Hence, considering errors, the sample size for this study was eight experts to evaluate the validity of the framework. Accordingly, the proposed framework was reviewed by conducting interviews with IA experts, which also include information security experts and eGovernment experts in Indonesia who have at least five years of experience.

4.2.2.3 Data Collection Process

The interviews with the experts were scheduled for over three weeks. The interviews were conducted in person and recorded using a mobile phone application. Each participant was asked to read the participant information sheet and sign the consent form at the beginning of the interview. The participant information sheet and consent form can be found in Appendix A and B.

Interview questions were semi-structured, which includes closed-ended and open-ended questions. Close-ended questions were aimed to attain experts' general information. The open-ended questions were purposed to attain expert opinions on the factors that have been identified and attain additional information on factors other than those already identified. The process took on average 30 minutes to finish an interview.

4.2.2.4 Data Analysis

In this study, data analysis by conducting thematic analysis was performed after the data was collected. The analysis started with a process of encoding information that produced a theme list (can be found in Appendix C), which is an idea that captures something important about the data in relation to the research question that represents a pattern in responses (Braun & Clarke, 2006). This was intended to be able to organise and systemised data in a complete and detailed way so that data can bring up a picture of the topics being studied. The themes were necessary for the process of interpreting the data. A node was also assigned to every dimension for the extent of experts' opinion, while all the characteristics and quality items of each node were classified as either "strongly disagree", "disagree", "agree", "strongly agree".

4.2.3 Practitioners survey

A survey was chosen to collect information to capture the knowledge of practitioners in the field of IA that include information security and eGovernment in Indonesia. The practitioner survey was conducted in the form of questionnaires aimed at confirming the proposed IA framework. The survey was conducted by distributing online questionnaires to practitioners in the field of IA that include information security and eGovernment. The respondents were required to take responsibility for reading and answering questions by using a self-administered survey.

4.2.3.1 Survey Design

The aim of the survey was to confirm the factors of the updated framework resulting from the expert review by performing a self-administered survey in an online questionnaire. The

questionnaire was divided into two parts. The first part was designed for collecting general information. The second part was designed for finding out your opinion about factors affecting information assurance implementation for eGovernment in Indonesia. The questionnaire featured four identified determinants on a four-point Likert scale with the following ratings: “strongly disagree” (=1); “disagree” (=2); “agree” (=3); “strongly agree” (=4). This is a "forced choice" scale and has an even number of answers and also eliminates the neutral (neither agree nor disagree) (Garland, 1991). The "forced choice" scale is not recommended to use in a survey that concerns a highly sensitive topic where a respondent may prefer to choose a neutral option (Cherdantseva, 2014). The reason this scale was chosen was that this study did not cover a highly sensitive personal topic. Moreover, a neutral option may be interpreted differently by participants and thus can hinder the accuracy of results and for the analysis, neutral answers provide little value (Cherdantseva, 2014). The full list of the survey questions is provided in Table 4.2.

The survey questions need to be tested before official use to ensure that the direction of completing the questionnaire and questions are clear and understandable as well as having an idea about how the structure and questions could be improved. A pre-test was thus conducted with 5 people. Two were professionals from different private sectors in Indonesia and three were from different government organisations in Indonesia. The pre-test produced two results: each questionnaire item was changed from a question sentence into a statement sentence and the editing of certain complicated sentences.

Table 4.2 Survey questions

Section A
Explanation: This section is used to collect your general information. Please consider all the options in each question carefully. 1. What industry sector do you work in? 2. Do you have any experience in the fields of Information Security, Information Assurance or eGovernment? □ Information Security □ Information Assurance □ eGovernment □ All of them □ Other _____ 3. How many years of experience do you have in the field you mentioned above? □ Less than two years □ Two years □ More than two years to five years □ More than five years
Section B

To what extent do you agree that the following factors affect information assurance implementation for eGovernment in Indonesia
Organisation Management
1. Leadership in the organisation is critical in the implementation of information assurance.
2. Commitment from the board level is critical for the achievement of information assurance through the initial planning.
3. Information assurance policy is important in providing management direction and a guide for meeting organisational objectives.
4. Legal aspects are important in identifying the organisation's legal obligation (statutory, regulatory, and contractual).
5. Compliance is necessary to ensure the organisation follows the legal aspects that apply to the organisation.
6. Senior management should periodically review (regarding the suitability, adequacy, and effectiveness) of the information assurance policy.
7. Senior management should continually improve the information assurance policy.
8. The information assurance shall be treated as a combination of the physical, procedural, personnel, and technical security.
9. The information assurance should be able to accommodate business needs.
10. Senior management must ensure roles in the organisation to confirm information assurance is in accordance with the policy.
11. Senior management must assign the responsibility for ensuring information assurance is in accordance with the policy.
12. Senior management must assign the authority to confirming information assurance is in accordance with the policy.
13. People who work in the organisation must be aware of the information assurance policy.
14. People who work in the organisation must be aware of its contribution to the effectiveness and performance of the information assurance.
15. All employees should be competent in their respective fields.
16. All employees of the organisation shall receive appropriate education as relevant for their job function.
17. All employees of the organisation shall receive appropriate training as relevant for their job function.
18. All employees of the organisation shall receive appropriate regular updates in the organisational policy as relevant for their job function.
Implementation Management
19. The organisation should understand the risk to the business information.
20. The organisation should undertake risk assessment to the business information.
21. The organisation should manage the risk to the business information.
22. Information security objectives must be determined relevant to the functions and levels.
23. Information security objectives must be consistent with the information security policy.
24. The organisation must ensure the plan of information security to comply with information security policy.
25. The organisation must ensure the implementation of information security to comply with information security policy.

26. The organisation must ensure the control of information security to comply with information security policy.
27. The organisation must ensure the update needed to comply with information security policy.
28. Internal audits need to be carried out to confirm whether the information assurance complies with the needs of the organisation and the international standards.
29. Performance evaluation need to be undertaken to ensure the effectiveness and maintenance of information assurance.
30. Monitoring need to be undertaken to evaluate the effectiveness and maintenance of information assurance.
31. Measurement need to be undertaken to evaluate the effectiveness and maintenance of information assurance.
32. Analysis need to be undertaken to evaluate the effectiveness and maintenance of information assurance.
33. The integrity and availability of information systems must be maintained during an incident or disaster.
34. Business continuity must be maintained and work as usual in the event of major failures of information systems.
Indonesian Context
35. Cultural issues in organisations in Indonesia can affect information assurance performance.
36. Cultural issues in organisations in Indonesia need to be considered in the implementation of information assurance.
37. Implementation of eGovernment requires good infrastructures to able to provide services as intended.
38. Information security process requires good infrastructures to be achieved in accordance with the security objectives.
39. Differences in geography in Indonesia, have resulted in the emergence of the gap in access to technology.
40. The gap in access to technology should be addressed regarding information assurance performance.
41. Trust must be established between government institutions.
42. Trust must be established between government and citizens.
43. The government should ensure that the user information is well protected.
44. The creation of an organisation like a National Cyber Agency to be in control of handling information security issues is required.
45. The creation of a division such as an information security division to be in control of handling information security issues within an organisation is required.
46. There must be coordination between institutions so that the duties of each institution do not overlap in protecting eGovernment information.
After Thoughts
47. Do you think the framework represents good fundamental guidelines for the implementation of information assurance for eGovernment in Indonesia?
48. Do you think the framework is useful in the implementation of information assurance for eGovernment in Indonesia?

49. Is there anything you would like to add?

4.2.3.2 Practitioners Survey Sample Size

To determine the sample size, the statistical power analysis programme, G* Power, was used to calculate the minimum sample size (Faul et al., 2009) as shown in Table 4.3. The tail was set as a two-tailed test, whereas is a method in which the critical area of a distribution is two-sided. It was chosen since this research use null-hypothesis testing and testing for statistical significance. Moreover, the effect size was 0.8, which means a large effect size (Cohen, 2013). The reason for this is because the difference between means is very substantial. Further, the margin of error must be determined (Banerjee et al., 2009). There are two error types that should be specified, which are alpha (α) and beta (β). Error type 1 is alpha that occurs when the true null hypothesis is rejected, while error type 2 is beta, which occurs when the null hypothesis is wrong but not rejected. Both errors need to be set to calculate the sample size needed for the study. In addition, the central limit theorem states that, as the sample size increases, which is usually defined as greater than 30, the sampling distribution will be normally distributed regardless of the shape of the population from which the sample was drawn (Field et al., 2013). For this research, it was decided that the minimum sample size was 30. The reason for this number was because the sample size of 30 covered both the calculation from the statistical power analysis programme and the central limit theorem.

Table 4.3 Minimum sample size

Tail(s)	2
Effect size	0.8
α err prob	0.05
Power (1-β err prob)	0.95
Minimum sample size	**23**

4.2.3.3 Data Collection Process

The method to conduct the survey was an online questionnaire as this method was convenient for respondents. Respondents were approached by email, personal contact, or forums and asked to complete the online questionnaire. The iSurvey application of the University of Southampton was used to generate and conduct the online survey. The first page of the questionnaire explained more about the research and its goals and shown them the consent form. If they agreed to take a part of this research, they should choose 'Yes' and press the bottom to the next page to answer the questions.

4.2.3.4 Data Analysis

Formal statistical procedure in the hypothesis test is by making two hypotheses and using statistical test to reject one hypothesis and accept or fail to reject the other hypothesis. The first hypothesis is commonly referred to as the null hypothesis because it states no difference between the populations of interest. The symbol for the null hypothesis is usually H_0. While the second hypothesis, or commonly known as the alternative hypothesis is symbolised by H_1, states that there is an effect or difference between populations.

In this research, the hypotheses were declared as the following:

H_0: There is no statistically significant difference from a mean of 2.5

H_1: There is a statistically significant difference from a mean of 2.5

All tests statistically provide a p-value which is equivalent to the possibility of obtaining observed differences. A p-value of 0.05 (5%) is generally considered to be sufficient to reject a null hypothesis. If the p-value is greater than 0.05, then the null hypothesis fails to be rejected. The p-value of 0.05 is called the significance level of the test (Field, 2013).

Reliability is the consistency of a series of measurements or a set of measuring instruments. Reliability is closely related to validity. Reliability or consistency of measurement is required to obtain valid results, but it is possible that reliability can be obtained without being valid. If validity is related to the feasibility of the interpretation of test results, then reliability relates to the consistency of test results. The reliability test was performed to determine the internal consistency of every test item in the survey questionnaire (Hair et al., 2006).

4.2.4 Case Studies

Once the instrument had been developed and ethical approval had been obtained, then it was presented and reviewed by five experts through interviews process. The aim of interviewing experts was to review the instrument measuring items and confirm the instrument. Once the instrument had been reviewed and refined, the confirmed instrument then used to conduct three case studies. Since the developed instrument is for government organisations, the case study will be conducted in public sector to predict similar results. The organisations where the case studies will be carried out are The Government Institution of Jakarta, The Government Institution of Bandung, and Pos Indonesia Bandung Region. The reason for choosing these three institutions is because these three institutions are categorised as government institutions and have implemented eGovernment with

varied time span. Therefore, with three case studies are undertaken, the case study will be literally replicated, which is accepted since the required is one type of replication, theoretically or literally (Yin, 2003).

The case studies will be based on qualitative focus groups with the participants will be from three management levels: strategic, tactical and operational, with the overall aim of the studies being to measure the IA implementation process status of the organisations using the confirmed instrument. Before conducting these case studies, permission will be requested and gained from the three organisations to conduct these studies. The experimental plan and procedure are as follow:

1. Each organisation would use the instrument to assess every dimension through the proposed questions and items.
2. The scores will be captured through a set of statements in the questionnaire.
3. The score for each component will be computed and will show the status of the IA implementation process.
4. Each participant will be asked to give their opinion regarding the result of IA implementation process status in their organisation.

Each participant will be asked to give their opinion and feedback regarding the instrument feasibility and practicality in measuring IA implementation process for eGovernment in Indonesia.

4.3 Ethical Approval

Prior to conducting the interviews, survey, and case studies, ethical approval was sought and obtained from the Ethics and Research Governance Committee, the University of Southampton; ERGO/FPSE/29459 for the interviews and survey and ERGO/FPSE/29459 for the case studies. All participants were informed about the study prior to the interview and survey. Consent was obtained from participants when they agreed to participate. Their participation was voluntary, and they could withdraw at any time. Participants were also assured of the anonymity and confidentiality of the data. All the collected data will be destroyed at the end of the study.

4.4 Summary

This chapter described the approach used to confirm the proposed framework and instrument. The research design for this study is a mixed-methods approach. The mixed-methods approach used is the triangulation method that combines qualitative method and quantitative method. A sequential procedure was performed in this study to apply the mixed-methods approach. Expert interviews,

which were the implementation of qualitative method, were carried out first to review the proposed framework. The results of the interviews were analysed using a thematic analysis. The second stage was a questionnaire survey, which was an implementation for the quantitative method. A series of statistical test was performed to test the quantitative data using SPSS. The reliability of the questionnaire was established using a Cronbach's Alpha coefficient. Further, in this chapter, the methodology to design the instrument was also explained. The instrument was developed using GQM approach. The instrument then was used in case studies to confirm its effectiveness in measuring IA implementation for eGovernment in the Indonesian context. Results and discussions are presented in the next chapters.

Chapter 5 Findings, results, and discussions of the expert interviews and practitioners survey

This chapter presents the results and discusses the confirmed IA framework for eGovernment in Indonesia. To confirm the framework, a mixed-methods approach was used which is a combination of qualitative and quantitative methods. Experts' interviews were conducted as a process to review the factors that have been identified. While practitioners survey conducted to confirm the factors that have been reviewed. Thematic analysis was used to analyse the interview results and interpret the data from the interviews. Furthermore, data from practitioners' survey was analysed using statistical methods with SPSS software. The summary at the end of the chapter presents the conclusions derived from both types of data obtained.

5.1 Findings of the expert interviews

This section presents and analyses the results of interviews conducted with experts in the fields of eGovernment, IA, and InfoSec. The data were obtained from semi-structured interviews with a total of eight experts from Indonesia. Expert interviews were carried out because it was important to review the factors identified in the literature review process. The interview process also allowed the emergence of new factors or recommendations from experts. This section is divided into the following: Experts Demographic, Analysis of Interviews, and Recommendations from Experts

5.1.1 Experts Demographic

As a first step, emails and personal messages were sent to 12 experts to inquire about their availability for an interview. Of the 12 experts, eight of them are willing to be interviewed. Furthermore, the eight experts, who are experts in eGovernment, IA, and InfoSec in Indonesia were interviewed. All participants have experience in eGovernment, IA, or InfoSec for at least five years. This means they are capable and have the capability of examining IA for eGovernment, especially in the present situation. Interviews conducted from August to September 2017 are face to face in Indonesia. A mobile application was used to record the interviews process. Prior to the interview, every participant was asked to give their consent. The following Table 5.1 presents the demographic of the experts.

Table 5.1 Overall description of experts

Variable		Frequency
Area of Expertise*	Information Assurance	3
	Information Security	4
	eGovernment	7
Job Domain	Academic	2
	Government	4
	Industry	2
Job Role	IA and InfoSec consultant	2
	Senior management in a government institution	2
	Researcher	4
Experience	5 years	3
	6-10 years	3
	More than 10 years	2

**Areas of expertise overlap*

5.1.2 Analysis of interviews

The reason behind for carrying out the expert interviews was to review the factors for IA implementation for eGovernment in Indonesia that have been identified in the literature review process and also to explore if additional factors exist. Semi-structured interviews were used which included closed-ended and open-ended questions. At the beginning of the interview, experts were asked about areas of expertise, job role and length of experience. The results can be seen in Table 5.1. Furthermore, the proposed framework is shown to the experts. Once they understood the framework, they were asked about the importance of the proposed factors. They were also asked about what factors had not been identified and recommendations for the framework. The purpose of these questions was to seek and clarify issues related to IA implementation for eGovernment in Indonesia. Data from interviews are then analysed and opinions from experts were interpreted. The results can be seen in the next section.

5.1.2.1 Organisational Management

After the experts understood the framework, they were asked about factors related to organisational management in the implementation of IA for eGovernment in Indonesia. The results of the interviews were clear; all experts agreed that factors related to organisational management are important in IA implementation. Among the most interesting statements from the respondents were:

- **Leadership and Commitment**

All experts reported the critical importance of leadership and commitment in the implementation of IA for eGovernment in Indonesia, as two experts stated:

> *"Leadership and commitment are very important and can affect the success or failure of the implementation of IA. Because if there is no commitment, then the implementation of IA will not be supported properly and can be stopped in the middle of the process"* (Expert 4).

> *"This factor is very important. Because in the government sector in Indonesia, the leaders are the one who makes policies. Then the policies will be broken down into a master plan, then it will be broken down more into strategic plans and then finally it needs a financial plan. This means that commitment to support from plan to finance is important to be able to do the implementation"* (Expert 8).

Some experts expressed that the interest and politics issue can interfere with the implementation of projects in the government sector including IA, as two experts stated:

> *"Sometimes if there is a change of leadership, there are rules and policies that are added or omitted because of interest or political matter. This impacts on changes in policy and affects the implementation of government project"* (Expert 5).

> *"Interest and politic make the commitment does not work. In the absence of a commitment, the planned projects, including IA, will not work properly"* (Expert 2).

Moreover, some experts stressed the importance of consistency of commitment for the success of the implementation of IA, as two experts stated:

> *"Commitment must be consistent from plan to finance. This means full support should be provided for the implementation process. The leaders should not just give orders and make plans but do not provide financial support"* (Expert 8).
> *"From experiences, in 2015 there are 18 projects in this local government but only three were successfully being implemented. This is because the leaders did not support and commit to the implementation. The three successful projects were due to their supportive and committed leaders"* (Expert 2).

- **Policy, Legal, and Compliance**

All experts supported the significant importance of policy, legal, and compliance in the implementation of IA for eGovernment in Indonesia. The policy is important in giving a direction, as stated by two experts below:

> *"Policy is a manifestation of commitment to force the organisation to implement what has been planned and to make the system work"* (Expert 2).

> *"Policy is important because policy will later determine the long-term plan, short-term plan, and work plan in government organisations. For example, a master plan will be the base of a strategic plan that will become programs"* (Expert 8).

Furthermore, the legal aspect is also important in providing legal protection to avoid dispute in the implementation process later, as stated by two experts below:

> "*Legal aspects need to be made so that there is no problem at the time of implementation later"* (Expert 3).

> *"When government instructions are issued for financing, legal aspects can be references for funds to be provided so the implementation can be undertaken"* (Expert 8).

Moreover, organisations must follow the policy and legal aspects that have been established, as stated by two experts below:

> *"Policy and legal aspects are essential for implementation to work out. In addition, organisations are required to follow the policies and legal aspects"* (Expert 7).

> *"In Indonesia, usually organisations already do the making of the policy and legal aspects and it is important to follow them. However, many organisations are yet to comply with the policy, legal aspects, or standards"* (Expert 3).

- **Management Review and Continual Improvement**

All experts agreed on the importance of management review and continual improvement in the IA implementation for eGovernment in Indonesia, as stated by two experts below:

> *"It is important to review policies. But in practice, the management review in government organisations is not undertaken by board level. The board will usually appoint senior management to review and then report to the board"* (Expert 2).

"There is a plan, monitoring, and evaluation here usually every three months. Technically, monitoring and evaluation are conducted and then there are reports of them. Furthermore, if there is something lack then improvement will be made" (Expert 3).

Moreover, some experts stated that periodic review should be undertaken at least once a year, as stated by two experts below:

"In this local government, there is a periodic review every five years. But I think it is not enough because it should be done at least once a year. Because if they do it every five years then the evaluation and improvement that must be undertaken later will be stacked" (Expert 5).

"If we talk about policies of the programs then there should be a review process and there should also be an annual report. It is intended as an evaluation for the next year improvement" (Expert 8).

- **Holistic Approach**

All experts supported the significant importance of the holistic approach in the implementation of IA for eGovernment in Indonesia. The unity of the physical, procedural, personnel and technical security shall be integrated into the process of implementing IA, as stated by three experts below:

"Holistic approach is important in the implementation of IA. it is similar to PPT (People, Performance, Technology) in organisations" (Expert 1).

"From my experience, all these elements must be well integrated into each other so that the implementation of IA can be successful" (Expert 7).

"All of them must be integrated. For example, if the procedure exists but is not physically supported, it will not work. And if the personnel exist but the procedure does not exist, nor will it work. So, all those components are mutually supportive for the implementation of IA" (Expert 8).

- **Business Alignment**

All experts reported the importance of business alignment in the implementation of IA for eGovernment in Indonesia, as three experts stated:

"Alignment of IA with the business is important and to achieve its organisation must pay attention to business needs, understand subject matters, suitable assessment, criteria and assess" (Expert 1)

"IA must be supportive and in harmony with business. And leadership factors are influential because that determines the organization's business direction policy" (Expert 3).

"The context of business here is programs. Therefore, IA must be aligned with the business as a supporter. Which means, IA acts as a supporter or part of a strategy to achieve the organisation's business goals" (Expert 8)

- **Organisational Roles, Responsibilities, and Authorities**

All experts supported the importance of organisational roles, responsibilities, and authorities in the implementation of IA for eGovernment in Indonesia, as stated by two experts below:

"The one responsible for determining the direction of the organisation and determining the policy is the board level. The function of top management (senior management) is to run PBRM (Plan Build Run Monitoring). Meanwhile, the function of the board is to do EDM (Evaluate Directing Monitoring). Therefore, each layer in the organisation has its own roles, responsibilities, and authorities" (Expert 1).

"This is important because within the organisation there should be people who carry out the main tasks and functions in accordance with their role in the organisation" (Expert 6).

In addition, every government employees in Indonesia are required by law to have their own functional positions in organisations, as stated by an expert below:

"State civil apparatus in Indonesia is required to legally have functional positions within organisations to define their roles, responsibilities, and authorities." (Expert 4).

As to become top management, it should be required that the people chosen has qualification or competency to do their job, as stated by an expert below:

"To become top management, it is needed to have qualifications and certifications. Because sometimes the chosen top management does not have qualifications or have different backgrounds, so they do not understand the task of their functional positions" (Expert 5).

- **Awareness, Education, and Training**

All experts supported the significant importance of awareness, education, and training in the implementation of IA for eGovernment in Indonesia. Awareness is important in the implementation, as stated by three experts below:

"All staff should be aware of what is being implemented (objectives). Because, although the policy already established, if there is no awareness it can lead to being a bottleneck in the bottom layer with the reason of not being accustomed to the policy" (Expert 2).

"Awareness is important, but in practice sometimes what happens is that not all layers are aware of the policy. Ideally, all layers should be aware of the policy, so they know what they do and the effects of their performance to the organisation" (Expert 4).

"Awareness is important. Even though the staff are not yet competent, they should be aware of the policy first. Competency can be achieved through education and training" (Expert 7).

Education and training are important to the employees so that they can have competency in their respective fields, as stated by two experts below:

"All staff should be competent. One way for judgment or justification of their competency is by certification through education or training" (Expert 8).

"All staff should be aware and competent in their field in order to do their jobs well, this can be achieved through education and training" (Expert 6).

Moreover, in Indonesia it is also required by law that all civil servants to have competency in their respective fields, as stated by an expert below:

"In the current government regulation, there is a law stipulating that every state civil apparatus must have competence in their respective field" (Expert 4).

5.1.2.2 Implementation Management

After being asked about factors related to organizational management, they were asked about factors related to implementation management in IA implementation for eGovernment in Indonesia. The result of the interview is clear; seven out of eight experts agreed that factors related to implementation management are important in IA implementation. Among the most interesting statements from the respondents were:

- **Risk Management**

All experts agreed on the importance of risk management in the IA implementation for eGovernment in Indonesia, as stated by two experts below:

> *"Organisations must perform risk management. Starting from risk assessment, risk management plan, and lastly risk treatment. This is important so that later in the implementation phase, organisations are ready to handle the risks"* (Expert 5).

> *"Risk management is important. However, risk cannot be eliminated but can be minimized. To minimize risk, it can be by transfer, accept, mitigation, or avoid"* (Expert 1).

Furthermore, even though risk management is important, in Indonesia most government organisations do not do the risk management process, as stated by two experts below:

> *"Organisations must be able to manage risk. However, in this institution, risk management is still not being undertaken. Because risk management is often deemed unimportant by the organisation"* (Expert 3).

> *"To be honest, in governmental institutions risk management is not a common thing to do. So, when it comes to implementing something, risks are often not being measured. Consequently, during the implementation phase, it often does not function properly because there is no risk management plan to handle risks"* (Expert 4).

Besides risks on the technical aspect, organisations also should be able to handle risks that may occur on other aspects such as policy and organisation culture, as stated by two experts below:

> *"Risks are not just related to changes in systems. There are also cultural risks. Because even though the system changes but the work culture might do not change. So, the government should be able to manage it"* (Expert 2).

> *"There should be treatments depending on the risks. For example, in the project management, risks are measured first and then strategic plan to handle it will be made. Then regarding programs, there are always risks that can occur, whether on technical aspect or policy aspect"* (Expert 8).

- **Security Objectives**

All experts reported the importance of security objectives in the implementation of IA for eGovernment in Indonesia, as two experts stated:

> ***"****Because the security objectives that have been made refers to the master plan, strategic plan, and become a program. So, it must be in accordance with the planned objectives"* (Expert 8)

> *"The security objectives are important so that the purpose of security can be defined from the beginning. And the objectives must be relevant to the levels and functions to be easily monitored and should be consistent with the policy"* (Expert 7).

Despite being considered as an important factor, government organisations in Indonesia often do not have security objectives, as stated by an expert below:

> *"Security objectives are important, especially for critical ones such as user data. Nevertheless, as previously said, same as risk management there is no security objectives in most government institutions. This is because security objectives are considered not critical by them"* (Expert 4).

Moreover, in the event of policy changes happen, security objectives should be able to adapt to it and change the objectives in accordance with the new policy, as stated by two experts below:

> *"Security objectives are important and indeed objectives must be determined. And to overcome the policy changes in the middle of the process then there should be control and update"* (Expert 1).

> "*Security objectives must in accordance with the initial planning at the beginning. And if there is a change in the policy, then the security objectives must adapt the changes"* (Expert 5).

- **Operations and Management**

All experts supported the importance of operations and management in the implementation of IA for eGovernment in Indonesia. The operations and management process is to ensure the implementation is in accordance with the plan, as stated by two experts below:

> *"Operation and management are important to ensure that everything must be in accordance with what is written in the master plan. Because in this case the plan has been*

stated in the policy. Thus, the implementation must be in accordance with what has been planned and controlled properly" (Expert 2).

"In practice, the plan becomes implementation programs. After that, there is evaluation in the form of control, and there should be an update process. In short, there should be a plan do check process" (Expert 8).

- **Performance Evaluation**

All experts agreed on the importance of performance evaluation in the IA implementation for eGovernment in Indonesia. The performance evaluation process is necessary to confirm if the IA implementation is well maintained, as stated by two experts below:

"Performance evaluation is important to ensure IA is maintained according to policy. Before performing a performance evaluation, the organisation should make characteristics for the evaluation first. Then usually before do the internal audit process, there is a self-assessment process first" (Expert 1).

"This factor is very influential. Because to confirm the success of IA implementation there must be monitoring process, evaluation, and must have its measurement, and analysis process. If there are no these processes, then the success of the IA implementation cannot be confirmed" (Expert 8).

- **Recovery and Continuity Management**

Seven experts agreed that recovery and business continuity management is important in the IA implementation for eGovernment in Indonesia. This is to ensure that eGovernment services still available in the event of incident or disaster, as stated by two experts below:

"Recovery and business continuity management is important because by having recovery and business continuity management then the business continuity can be assured. This institution already has implemented this, as for example data from this institution has been backed up outside the city" (Expert 3).

"It is important, so the organisation could cope with incidents that might occur. Because if there is an incident that makes services disturbed then there must be countermeasures plan to keep the services running" (Expert 4).

In Indonesia, there is a law that requires every organisation that provides electronic-based services to have a business continuity plan, as stated by one expert below:

"This factor is important, even in Indonesia, there is a government regulation governing any organisation that runs electronic-based services must have a business continuity plan" (Expert 6).

One expert stated that even recovery and continuity management is important, the configuration management database is more important, as stated below:

"Configuration Management Database (CMDB) is more important. Inside CMDB there is human aspects and a map. There can be mapped if a process is disturbed then what might be interrupted" (Expert 1).

5.1.2.3 Indonesian Context

Lastly, they were asked about factors related to the Indonesian context in IA implementation for eGovernment in Indonesia. The result of the interview is clear; all experts agreed that factors related to the Indonesian context are important in IA implementation. Among the most interesting statements from the respondents were:

- **Cultural Issues**

All experts supported the importance of cultural issues in the implementation of IA for eGovernment in Indonesia. People habits can affect their performance and affect their organisation, as stated by an expert below:

"Cultural issues are very influential because culture cannot change quickly. Like when the leadership changes, then the policy also changes. Then despite the standard operating procedure is already established, but they do not do it. So, the consideration is the existing habits in Indonesia is influential. Another example is let's say everything is complete, such as rules, policies, but still they do not do it, it is because of habits of the people in Indonesia. So cultural issues are influential" (Expert 8).

Another issue in Indonesia is the problem of resistance to change, as stated by two experts below:

"When they are used to the old way and this becomes a culture or habit then when the new system is being implemented, there is a difficulty to change the culture and resulting in resistance to change. Resistance will also depend on their interests, such as if there are interests from a party. Then from the management perspective, for example a process flow for the same process in an agency with another agency is different. So, if a uniformity will be undertaken, it will change the culture of their work and consequently that sometimes resistance arises" (Expert 2).

"Resistance to change often arises due to habit. The solution can be from the top management that forces with policy. Because with the policy which has goals for the organisation, it is inevitably must be undertaken by all parties" (Expert 4).

Furthermore, in Indonesian government institutions usually, there is no culture of sharing. It happens due to their habit and bureaucracy, as stated by two experts below:

"The habits of Indonesians can affect organisational performance and IA. The bureaucracy in government institutions is so complicated resulting in difficulty in data sharing. Thus, there must be rules that force to change the culture" (Expert 6).

"Although communication between institutions already exists, problems arise in the people. Like there are not willing to share and prefer to use conventional way. It is due to many people still have old-fashioned habits" (Expert 5).

- **Infrastructures Development**

All experts reported the critical importance of infrastructure development in the implementation of IA for eGovernment in Indonesia, as two experts stated:

"Infrastructures are important in supporting the implementation of IA. Although infrastructures development in Indonesia has not been evenly distributed. In addition, the government should have its own infrastructure. It is not recommended to use a third party. It is due to the infrastructure for government, thus safe and secure and its privacy must be guaranteed" (Expert 5).

"If the infrastructures are not good then it cannot support the implementation of IA or eGovernment. And to handle it there must be infrastructures development" (Expert 8).

- **Digital Divide**

All experts supported the importance of the digital divide in the implementation of IA for eGovernment in Indonesia. The digital divide can occur due to technological infrastructure gap caused by geographical location that is not reached by technological developments, as stated by two experts below:

"If for example, the central government wants to implement into each region, digital divide is very influential because the achievement of each region is different. Bandung may be okay because of good infrastructure, Jakarta may be okay, but we do not know what about Papua and what about Kalimantan. Therefore, this gap is influential. Let alone in a big scope, for

example in a city there is also a gap between an institution with another institution. Also in Indonesia usually, the government officers are old and do not understand technology so that can become a bottleneck" (Expert 2).

"Gap in the acceptance of technology in Indonesia is very big. Access to technology is uneven between regions and it becomes our problem too. Therefore, the government has a national priority program. This program refers to the plan of government program in supporting research activities for disadvantaged areas. Namely appropriate technologies for equity of technology" (Expert 3).

Furthermore, the digital divide can also occur because of lack of skills and digital literacy even though they have the necessary equipment and access to the technology, as stated by two experts below:

"Gap in technology or uneven access to information will result in uneven competence. And also, each region has a different vision of technology, so it will affect the achievement of technology" (Expert 8).

"I have experience in Sumatra. In order just to implement information systems is already difficult, let alone IA. This is because it relates to the availability of infrastructure. Some regions are not reached by technology developments. Whereas the people of the regions actually wanted and interested in technologies, but infrastructures and technological aspects have not been available" (Expert 4).

- **Trust and Privacy**

All experts agreed on the importance of trust and privacy in the IA implementation for eGovernment in Indonesia. Public trust can be obtained if the government is able to protect its data, as stated by one expert below:

"Security and privacy must be guaranteed so citizens can trust the government. And there must be a collaboration factor between citizen and government" (Expert 5).

Moreover, the government should be able to guarantee the privacy of the citizens' data, as stated by two experts below:

"The privacy issue is crucial. For example, electronic resident identity card, it is a strategic data. However, the server is not in Indonesia. Then, the infrastructures do not conform to the specified specifications, so the security is not guaranteed. If the data is stored in a third-

party server, then the data can be used the party who is not authorized or misused. It could be mined and exploited by others" (Expert 8).

"The government should be able to protect citizens' privacy. There is a regulation of Minister of Communications and Informatics, which reads every provider of electronic data, must be able to protect user data. Not long ago there was a problem in electronic resident identity card and a mobile operator" (Expert 6).

- **Organisational Structures**

All experts supported the importance of organisational structures in the implementation of IA for eGovernment in Indonesia. The establishment of an agency to deal with national security issues is necessary, as stated by one expert below:

"To handle security problems, Indonesia just established the National Cyber and Crypto Agency to filter out information and handle security problems. In Indonesia, there are several agencies that monitor the internet, but they work alone. Therefore, when there are incidents and reports, they do not know what to do. Thus, the purpose of the establishment of National Cyber and Crypto Agency is to function as an agency that overshadows and coordinate other agencies" (Expert 6).

Although it is important to have an agency that deals with national security issues, still in every organisation there should also be a division dealing with security issues, as stated by two experts below:

"National security agency is important and needs to be improved like KISA in Korea. Nevertheless, if one organisation has to deal with all information security issues then I do not agree. Because information security must be maintained by all organisations" (Expert 1).

"Although there should be a national-scale organisation, at the local level there should also be a division in charge of combating security issues" (Expert 6).

- **Coordination**

All experts agreed on the importance of coordination in the IA implementation for eGovernment in Indonesia. Coordination between agencies dealing with security issues is important, as stated by two experts below:

"Although there are agencies that deal with security issues, in practice agencies like ID-SIRTI and CERT-ID sometimes do overlapping work. Even so the government has made an effort to arrange both to clear its responsibilities and scope" (Expert 4).

"Coordination needs to be done so that no more additional work or overlap. Thus, it is no longer happen that agencies do the work that has been done" (Expert 8).

5.1.3 Recommendations from experts

Besides providing feedback on the framework, the respondents also gave their recommendations to enhance the proposed framework as follows:

1. Experts 1, 3 and 7 gave the recommendation to add to the organisational structure factor, which not only includes a national scale organisation, but also every institution needs to have its own division responsible for security issues.
2. Experts 4, 7, and 8 recommended carrying out dissemination and collaboration for a successful implementation of the IA.
3. Experts 4, 5, 7, and 8 gave recommendations to focus on cultural issues for the successful implementation of IA in Indonesia.
4. Expert 5 recommended adding political and economic issues to the framework.

Of the several recommendations, after consideration, only one recommendation was considered since the rest is already covered by the factors. The fact that most recommendations given by experts already exist in the framework could be due the lack of clearance during the presentation of the framework and the explanation as well as the scope of each factor. Moreover, the presentation only introduced the factors of the framework, but it didn't present the factors identified from the best practices and literature that were used in the development of this framework.

The only recommendation that taken into account was the number one, which is to expand the scope of the description of the organisational structure factor. Because the implementation process of IA depends on each institution, therefore every institution needs to have a division that deals with security issues. For recommendation number 2 that is socialization and collaboration, it is already included in awareness, education, and training factors that focus on the capability of employees. Furthermore, the recommendation on cultural issues has also already covered in the proposed framework. Finally, for both economic and political factors, these two factors are already embedded in leadership and commitment factors, where funding for IA implementation depends

on the commitment of the leader and commitment of the leader is also be influenced by political issues.

5.2 Findings of the survey

This section presents the findings of the practitioners' survey. Period of data collection through the online questionnaire was from October to December 2017. The tool used was an online-based website questionnaire. The questionnaire was distributed to a total of 50 respondents as well as forums, and the total number that filled in the questionnaire was 32 respondents. All participants come from various industries in Indonesia. Furthermore, each participant has a minimum of two years of experience in the field of IA, eGovernment, or InfoSec. The reason for conducting the survey was to confirm the proposed framework. Furthermore, this section consists of the respondents' demographics as well as the survey analysis and lastly the reliability test.

5.2.1 Respondents' demographic

The participants' demographic data were collected in order to establish whether they could take part in the study. Consideration was only given to participants who have experience in the field of IA, eGovernment, or InfoSec for two years or more. The job domains of the participants were very diverse, ranging from IT industry to academic. Table 5.2 below provides a summary of the practitioners' demographic details.

Table 5.2 Overall description of practitioners

Variable		Frequency
Area of Expertise*	Information Assurance	8
	Information Security	19
	eGovernment	15
Job Domain	Academic	9
	Government	9
	IT Industry	8
	Research	3
	Others	3
Experience	2 years	4
	2-5 years	23
	More than 5 years	5

**Areas of expertise overlap*

5.2.2 Analysis of the survey

This sub-section provides the results of the survey. The quantitative data was obtained using an online questionnaire. All the respondents are practitioners in Indonesia who are working in information security, information assurance or eGovernment field with more than 2 years experiences. The aim of the survey was to confirm the proposed framework. The closed-ended questions were proposed to refine the factors in the framework. The closed-ended questions in this section were involved forty-six items, where one to six were stated about each factor. A four-point Likert Scale (strongly agree, agree, disagree, strongly disagree) was used. The One-Sample T-test was used to analyse as a statistical test the results of the quantitative data. Table 5.3 presents the coding and description of the survey questions.

Table 5.3 Survey questions and factors code

Factors	Code
Organisational Management	
Leadership and Commitment	OF1
1. Leadership in the organisation is critical in the implementation of information assurance.	OF1.1
2. Commitment from the board level is critical for the achievement of information assurance through the initial planning.	OF1.2
Policy, Legal, and Compliance	OF2
3. Policy is important in providing management direction and a guide for meeting organisational objectives.	OF2.1
4. Legal aspects are important in identifying the organisation's legal obligation (statutory, regulatory, and contractual).	OF2.2
5. Compliance is necessary to ensure the organisation follows the legal aspects that apply to the organisation.	OF2.3
Management Review and Continual Improvement	OF3
6. Senior management should periodically review (regarding the suitability, adequacy, and effectiveness) of the information assurance policy.	OF3.1
7. Senior management should continually improve the information assurance policy.	OF3.2
Holistic Approach	OF4
8. The information assurance shall be treated as a combination of the physical, procedural, personnel, and technical security.	OF4.1
Business Alignment	OF5
9. The information assurance should be able to accommodate business needs.	OF5.1
Organisational Roles, Responsibilities, and Authorities	OF6
10. Senior management must ensure roles in the organisation to confirm information assurance is in accordance with the policy.	OF6.1
11. Senior management must assign the responsibility for ensuring information assurance is in accordance with the policy.	OF6.2
12. Senior management must assign the authority to confirming information assurance is in accordance with the policy.	OF6.3

Awareness, Education, and Training	OF7
13. People who work in the organisation must be aware of the information assurance policy.	OF7.1
14. People who work in the organisation must be aware of its contribution to the effectiveness and performance of the information assurance.	OF7.2
15. All employees should be competent in their respective fields.	OF7.3
16. All employees of the organisation shall receive appropriate education as relevant for their job function.	OF7.4
17. All employees of the organisation shall receive appropriate training as relevant for their job function.	OF7.5
18. All employees of the organisation shall receive appropriate regular updates in the organisational policy as relevant for their job function.	OF7.6
Implementation Management	
Risk Management	IF1
19. The organisation should understand the risk to the business information.	IF1.1
20. The organisation should undertake risk assessment to the business information.	IF1.2
21. The organisation should manage the risk to the business information.	IF1.3
Security Objectives	IF2
22. Information security objectives must be determined relevant to the functions and levels.	IF2.1
23. Information security objectives must be consistent with the information security policy.	IF2.2
Operations and Management	IF3
24. The organisation must ensure the plan of information security to comply with information security policy.	IF3.1
25. The organisation must ensure the implementation of information security to comply with information security policy.	IF3.2
26. The organisation must ensure the control of information security to comply with information security policy.	IF3.3
27. The organisation must ensure the update needed to comply with information security policy.	IF3.4
Performance Evaluation	IF4
28. Internal audits need to be carried out to confirm whether the information assurance complies with the needs of the organisation and the international standards.	IF4.1
29. Performance evaluation need to be undertaken to ensure the effectiveness and maintenance of information assurance.	IF4.2
30. Monitoring need to be undertaken to evaluate the effectiveness and maintenance of information assurance.	IF4.3
31. Measurement need to be undertaken to evaluate the effectiveness and maintenance of information assurance.	IF4.4
32. Analysis need to be undertaken to evaluate the effectiveness and maintenance of information assurance.	IF4.5
Recovery and Continuity Management	IF5
33. The integrity and availability of information systems must be maintained during an incident or disaster.	IF5.1

34. Business continuity must be maintained and work as usual in the event of major failures of information systems.	IF5.2
Indonesian Context	
Cultural Issues	CF1
35. Cultural issues in organisations in Indonesia can affect information assurance performance.	CF1.1
36. Cultural issues in organisations in Indonesia need to be considered in the implementation of information assurance.	CF1.2
Infrastructures Development	CF2
37. Implementation of eGovernment requires good infrastructures to able to provide services as intended.	CF2.1
38. Information security process requires good infrastructures to be achieved in accordance with the security objectives.	CF2.2
Digital Divide	CF3
39. Differences in geography in Indonesia, have resulted in the emergence of the gap in access to technology.	CF3.1
40. The gap in access to technology should be addressed regarding information assurance performance.	CF3.2
Trust and Privacy	CF4
41. Trust must be established between government institutions.	CF4.1
42. Trust must be established between government and citizens.	CF4.2
43. The government should ensure that the user information is well protected.	CF4.3
Organisational Structures	CF5
44. The creation of an organisation like a National Cyber Agency to be in control of handling information security issues is required.	CF5.1
45. The creation of a division such as an information security division to be in control of handling information security issues within an organisation is required.	CF5.2
Coordination	CF6
46. There must be coordination between institutions so that the duties of each institution do not overlap in protecting eGovernment information.	CF6.1

5.2.3 Practitioners' evaluation of the proposed framework

Details of practitioners' responses regarding the importance of the factors in the proposed framework are provided in the following subsections.

1. Organisational Management

Table 5.4 presents the frequency of organisational management factors. There are eighteen items divided by eight factors of organisational management that affect the implementation of information assurance for eGovernment in Indonesia. Of the 32 respondents, 81.3% strongly agree that the Leadership and Commitment factor is part of organisational management that is affecting the implementation of information assurance for eGovernment in Indonesia and 71.9% responded 'strongly agree' for OF1.1 and OF2.2. The 68.8% respondents responded if Policy, Legal, and

Compliance is a factor that is affecting the implementation of information assurance for eGovernment in Indonesia responded 'strongly agree' to OF2.1 and 71.9% to OF2.2, while the remaining 31.2% responded 'agree' to OF2.3. The third factor is Holistic Approach, 50% respondents responded, 'strongly agree' to OF3.1 and 56.3% responded 'agree' to OF3.2 which means this factor is affecting the implementation of information assurance in organisational management, while one respondent stated 'disagree' to both OF3.1 and OF3.2. For the OF4.1, 65.6% of respondents stated, 'strongly agree' and the other 34.4% stated 'agree' if this factor from the organisation management affects the implementation of information assurance. Moreover, 68.8% respondents stated 'strongly agree' to OF5.1. Ultimately, 50% and 59.4% of respondents responded 'agree' to OF6.1 and OF6.2 respectively, while 53.1% responded 'strongly agree' to OF6.3 regarding if Organizational Roles, Responsibility, and Authorities is affecting the implementation of information assurance for eGovernment in Indonesia. Awareness, Education, and Training factor is seen as an important factor from organisational management that affect the implementation of information assurance in Indonesia with 62.5% respondents responded 'strongly agree' if this factor is important on both OF7.1 and OF7.2. While 59.4% and 65.6% of the respondents responded 'strongly agree' to OF7.3, OF7.4 and OF7.5, OF7.6 respectively.

Table 5.4 Organisational Management factors frequency

Factors	**Frequency (Percentage)**				
	Strongly Disagree	Disagree	Agree	Strongly Agree	**Total**
OF1.1	0%	0%	18.7%	81.3%	32
OF1.2	0%	0%	28.1%	71.9%	32
OF2.1	0%	0%	31.2%	68.8%	32
OF2.2	0%	0%	28.1%	71.9%	32
OF2.3	0%	0%	59.4%	40.6%	32
OF3.1	0%	3.1%	46.9%	50%	32
OF3.2	0%	3.1%	56.3%	40.6%	32
OF4.1	0%	0%	34.4%	65.6%	32
OF5.1	0%	0%	31.2%	68.8%	32
OF6.1	0%	3.1%	50%	46.9%	32
OF6.2	0%	0%	59.4%	40.6%	32
OF6.3	0%	0%	46.9%	53.1%	32
OF7.1	0%	0%	37.5%	62.5%	32
OF7.2	0%	0%	37.5%	62.5%	32
OF7.3	0%	0%	40.6%	59.4%	32
OF7.4	0%	0%	40.6%	59.4%	32
OF7.5	0%	0%	34.4%	65.6%	32
OF7.6	0%	0%	34.4%	65.6%	32

2. Implementation Management

Table 5.5 shows the frequency of implementation management factors in terms of their influence on the implementation of information assurance for eGovernment in Indonesia. A total of five factors divided into 16 items are included in the practitioners' questions. Of the 32 participants, 78.1% stated 'strongly agree' if Risk Management is a factor that is affecting the implementation of information assurance for eGovernment in Indonesia to IF1.1, while 71.9% responded the same to IF1.2, and 68.8% also gave the same response to IF1.3. Furthermore, the second factor of Implementation Management which is Security Objectives is also affecting the implementation of information assurance with total respondents who stated, 'strongly agree' to IF2.1 and 'agree' to IF2.2 is 53.1% and 56.3% respectively. Moreover, 50% of respondents strongly agree to both IF3.1 and IF3.3 regarding Operations and Management factor affects the implementation of information assurance in for eGovernment Indonesia, with the other 56.3% chose 'strongly agree' to IF3.2. An average of more than 50% of respondents chose 'strongly agree' to IF4.1, IF4.2, IF4.3, IF4.5 which are items for Performance Evaluation. Meanwhile, 56.3% of respondents chose 'agree' to IF4.4. A total of 78.1% and 65.6% respondents responded, 'strongly agree' to IF5.1 and IF5.2 which means Recovery and Continuity Management influences the implementation of information assurance.

Table 5.5 Implementation Management factors frequency

Factors	**Frequency (Percentage)**				
	Strongly Disagree	Disagree	Agree	Strongly Agree	**Total**
IF1.1	0%	0%	21.9%	78.1%	32
IF1.2	0%	0%	28.1%	71.9%	32
IF1.3	0%	0%	31.2%	68.8%	32
IF2.1	0%	0%	46.9%	53.1%	32
IF2.2	0%	0%	56.2%	43.8%	32
IF3.1	0%	0%	50%	50%	32
IF3.2	0%	0%	43.7%	56.3%	32
IF3.3	0%	0%	50%	50%	32
IF3.4	0%	0%	43.7%	56.3%	32
IF4.1	0%	0%	46.9%	53.1%	32
IF4.2	0%	0%	43.7%	56.3%	32
IF4.3	0%	0%	46.9%	53.1%	32
IF4.4	0%	0%	56.3%	43.7%	32
IF4.5	0%	0%	31.2%	68.8%	32
IF5.1	0%	0%	21.9%	78.1%	32
IF5.2	0%	0%	34.4%	65.6%	32

3. Indonesian Context

In the practitioner's survey, respondents were also asked about the factors for the Indonesian context. There are six factors that are included in the Indonesian context that affect the

implementation of information assurance for eGovernment in Indonesia which are spread out into 12 items. The first factor is Cultural Issues, 71.9% and 65.6% of respondents chose 'strongly agree' to CF1.1 and CF1.2 respectively, which gives meaning if the factor is influential in the implementation of information assurance in the context of Indonesia, while there is one respondent who chose 'disagree' to CF1.1 and two respondents who chose 'disagree' to CF1.2. For the Infrastructure Development factor, 62.5% of respondents responded, 'strongly agree' and 37.5% stated 'agree' to both CF2.1 and CF2.2 regarding if this factor affects the implementation of information assurance for eGovernment in the Indonesian context. A total 65.6% and 56.3% of respondents chose, 'strongly agree' to CF3.1 and CF3.2 respectively which means the Digital Divide factor is also influential in the implementation of information assurance, while there are only two respondents who disagree to CF3.1 and one respondent who disagree to CF3.2. The Trust and Privacy factor in influencing the implementation of IA for eGovernment in the Indonesian context is confirmed by 53.1% of the practitioners who were choosing 'agree' to CF4.1, while the other 62.5% and 65.6% respondents were choosing 'agree' to CF4.2 and CF4.3 respectively. Furthermore, 53.1% of the respondents stated, 'strongly agree' and 46.9% stated agree' to CF5.1 and CF5.2. It means the Organisational Structures factor influence the implementation of information assurance for eGovernment in the Indonesian context despite there one respondent who chose 'disagree' to CF5.1 and two respondents who chose 'disagree' CF5.2. Lastly, 65.6% of respondents 'strongly agree' if the Coordination factor affects the implementation of information assurance. Table 5.6 presents the frequency of Indonesian Context factors in terms of their influence on the implementation of information assurance for eGovernment in Indonesia.

Table 5.6 Indonesian Context factors frequency

Factors	**Frequency (Percentage)**				
	Strongly Disagree	Disagree	Agree	Strongly Agree	**Total**
CF1.1	0%	3.1%	25%	71.9%	32
CF1.2	0%	6.3%	28.1%	65.6%	32
CF2.1	0%	0%	37.5%	62.5%	32
CF2.2	0%	0%	37.5%	62.5%	32
CF3.1	0%	6.3%	28.1%	65.6%	32
CF3.2	0%	3.1%	40.6%	56.3%	32
CF4.1	0%	0%	53.1%	46.9%	32
CF4.2	0%	0%	37.5%	62.5%	32
CF4.3	0%	0%	34.4%	65.6%	32
CF5.1	0%	3.1%	43.8%	53.1%	32
CF5.2	0%	6.2%	46.9%	46.9%	32
CF6.1	0%	0%	34.4%	65.6%	32

The One-Sample t-test was used to analyses as a statistical test. The test makes it possible to assess the distribution of mean value. The hypothesised mean (μ_0) set as 2.5 and the test value was defined as 2.5 on the four-point Likert scale for security factor, which ranged from 4 (Strongly Agree) to 1 (Strongly Disagree). The hypotheses for testing each factor are as follows:

H_0: There is no statistically significant difference from a mean of 2.5

H_1: There is a statistically significant difference from a mean of 2.5

The statistical significant level alpha is $\alpha = 0.05$. The null hypothesis (H_0) is rejected if the probability (P-value) of question is < a = 0.05. The factor is statistically significant if the p-value < 0.05, otherwise, the factor is not statistically significant. In this study, Bonferroni correction was applied for controlling the false positive finding by dividing alpha (α= 0.05) by the number of items involved in the questionnaire. For this study, the adjusted P-value is defined as below:

P-value = (α/n)

= 0.05/46

= 0.001

Which means, the factor is statistical significance if the p-value < 0.001. Otherwise, the factor is not statistically significant. It means that all the factors are important in the implementation of IA for eGovernment in Indonesia. The results also give an indication that the results of practitioners survey are in accordance with the expert interview which means all the experts and practitioners who participated in the interview and the survey agreed with the importance of the factors and there was no reason to remove any of them.

Table 5.7, shows the analysis results of questionnaire for each factor. From the questionnaire results, it can be seen that the attitude of all categories and its factors are all significant in affecting information assurance implementation. All the results of the items show a mean >2.5 and p-value <0.001, therefore, H_0 is rejected and the H_1 is accepted. It means that all the factors are important in the implementation of IA for eGovernment in Indonesia. The results also give an indication that the results of practitioners survey are in accordance with the expert interview which means all the experts and practitioners who participated in the interview and the survey agreed with the importance of the factors and there was no reason to remove any of them.

Table 5.7 One sample t-test for the practitioners' survey

Category	Variable	Items	Test Value = 2.5		
			Mean	Sig. (2-tailed)	Results
Organ	OF1	OF1.1	3.81	<0.001	Statistically significant

		OF1.2	3.72	<0.001	Statistically significant
	OF2	OF2.1	3.69	<0.001	Statistically significant
		OF2.2	3.72	<0.001	Statistically significant
		OF2.3	3.40	<0.001	Statistically significant
	OF3	OF3.1	3.47	<0.001	Statistically significant
		OF3.2	3.38	<0.001	Statistically significant
	OF4	OF4.1	3.66	<0.001	Statistically significant
	OF5	OF5.1	3.69	<0.001	Statistically significant
	OF6	OF6.1	3.44	<0.001	Statistically significant
		OF6.2	3.41	<0.001	Statistically significant
		OF6.3	3.53	<0.001	Statistically significant
	OF7	OF7.1	3.63	<0.001	Statistically significant
		OF7.2	3.63	<0.001	Statistically significant
		OF7.3	3.59	<0.001	Statistically significant
		OF7.4	3.59	<0.001	Statistically significant
		OF7.5	3.66	<0.001	Statistically significant
		OF7.6	3.66	<0.001	Statistically significant
Implementation Management	IF1	IF1.1	3.78	<0.001	Statistically significant
		IF1.2	3.72	<0.001	Statistically significant
		IF1.3	3.69	<0.001	Statistically significant
	IF2	IF2.1	3.53	<0.001	Statistically significant
		IF2.2	3.44	<0.001	Statistically significant
	IF3	IF3.1	3.50	<0.001	Statistically significant
		IF3.2	3.56	<0.001	Statistically significant
		IF3.3	3.50	<0.001	Statistically significant
		IF3.4	3.56	<0.001	Statistically significant
	IF4	IF4.1	3.53	<0.001	Statistically significant
		IF4.2	3.56	<0.001	Statistically significant
		IF4.3	3.53	<0.001	Statistically significant
		IF4.4	3.44	<0.001	Statistically significant
		IF4.5	3.69	<0.001	Statistically significant
	IF5	IF5.1	3.78	<0.001	Statistically significant
		IF5.2	3.66	<0.001	Statistically significant
Indonesian Context	CF1	CF1.1	3.69	<0.001	Statistically significant
		CF1.2	3.59	<0.001	Statistically significant
	CF2	CF2.1	3.63	<0.001	Statistically significant
		CF2.2	3.63	<0.001	Statistically significant
	CF3	CF3.1	3.59	<0.001	Statistically significant
		CF3.2	3.53	<0.001	Statistically significant
	CF4	CF4.1	3.47	<0.001	Statistically significant
		CF4.2	3.63	<0.001	Statistically significant
		CF4.3	3.66	<0.001	Statistically significant
	CF5	CF5.1	3.50	<0.001	Statistically significant
		CF5.2	3.41	<0.001	Statistically significant

	CF6	CF6.1	3.66	<0.001	Statistically significant

5.2.4 Reliability test

This study employed Cronbach's Alpha to guarantee the reliability of the items and to effectively measure the factors. The SPSS software used to carry out Cronbach's Alpha test. Table 5.8 summarises the reliability test used to test the factors; Cronbach's alpha measured internal consistency for Organisational Management was 0.891, Implementation Management was 0.871, Indonesian Context was 0.721. According to Bryman and Cramer (2001), a Cronbach's alpha around 0.7 shows that the measured items are considered to have good internal consistency, while a Cronbach's alpha around 0.8 or above is considered as a very good internal consistency.

Table 5.8 Reliability statistics of the questionnaire

Reliability Statistics			
Category	Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
Organisational Management	0.891	0.891	18
Implementation Management	0.871	0.870	16
Indonesian Context	0.721	0.733	12

5.3 Discussion of the findings

This section presents a discussion of the findings. The experts reviewed the proposed factors and confirmed them as important for IA. Moreover, the survey confirmed that the factors are essential for the implementation of IA for eGovernment in Indonesia.

All experts agree that all factors in the Organisational Management category affect the implementation of IA for E-Government in Indonesia. Furthermore, experts emphasise on the importance of the Leadership and Commitment factor, because the implementation depends on the leaders and therefore, their influence and commitment will have an impact on the success or failure of the IA implementation.

Furthermore, seven experts agree that all the factors in the Implementation Management category affect the implementation of IA. Except for one expert, that states disagree with the Recovery and Continuity Management factor and states that the Configuration Management Database (CMDB) is more important. However, despite that, the expert agrees if the rest of the factors are important for the implementation of IA. Therefore, it can be concluded that all the factors of this category are significant and affect the implementation of IA.

Moreover, the factors in the Indonesian Context category affect the implementation of IA as stated by experts. All experts agree that all factors in this category are important and affect the implementation of IA for eGovernment in Indonesia. Additionally, experts also emphasise on the Cultural Issues and Digital Divide factors. These factors need more attention since Indonesia has a distinctive approach that emerges from its geographical situation and cultural context as a developing country in the South East Asia region. All in all, it can be concluded that all the experts and who participated in the interview agreed with the importance of the factors and there was no reason to remove any of them.

Additionally, from the results of the expert interviews and practitioners survey, it was found that there are several factors that need to be prioritised. The results of expert interviews revealed that Leadership and Commitment, Management Review and Continual Improvement, Recovery and Continuity Management, Digital Divide, and Cultural Issues need to be prioritised. Meanwhile, the results of practitioners survey unveiled that Leadership and Commitment, Risk Management, Recovery and Continuity Management are the factors that need to be prioritised with the highest respondents who responded 'strongly agree' to the importance of these factors with percentage of 76.6%, 72.9%, and 71.8%, respectively.

Besides providing feedback on the framework, the respondents also gave their recommendations to enhance the proposed framework. Of the several recommendations, after consideration, only the one recommendation was considered, which is to expand the scope of the description of the organisational structure factor.

Further, the findings of the questionnaire show that all factors influence the implementation of IA for eGovernment in Indonesia. Using statistical testing, all items in the questionnaire are confirmed. In terms of the mean scores yielded by the quantitative questionnaire analysis, the values ranged from 3.38 to 3.91; this showed that the factors have a substantial effect. Moreover, in relation to the statistical results, after studying the questionnaire findings, it was concluded that all factors are statistically significant. In sum, the respondents were in agreement that all factors are vital and ought to be taken into account when organisations are attempting to achieve IA.

In addition, a reliability test was carried out to measure the internal consistency using Cronbach's Alpha test. The results show that the internal consistency for Organisational Management and Implementation Management categories is very good. Meanwhile, the Indonesian Context category has good internal consistency.

Moreover, during the upgrade examination, there is a recommendation from the reviewer to change the name of the Indonesian Context category. The reason is that since the whole framework is supposed for the Indonesian context, not only the said category.

Hence, some improvements were undertaken on the framework, based on the expert interviews' findings and suggestions. Two improvements were applied as follows:

1. Expand the scope of the description of organisational structure factor from the creation of a national scale organisation to deal with security issues into the creation of a division within institution. The reason is that the implementation process of IA depends on each institution, therefore every institution needs to have a division that deals with security issues.
2. Change the name of the Indonesian Context category. The Indonesian Context category was renamed to Social Management category. The reason is since not only the said category but the whole framework is supposed for the Indonesian context. With the rename of the category, the Infrastructure factor moved was from Social Management category to Implementation Management category. This is because the scope and definition of the factor are more suitable to be placed in the Implementation Management category. Table 5.9 shows the confirmed framework for IA implementation for eGovernment in Indonesia government organisations.

From the discussions above, it can be concluded that this study has identified factors affecting the implementation of IA for eGovernment in Indonesia. Furthermore, by identifying factors which are influenced by IA standard-based frameworks, IA critical success factors, and challenges within the Indonesian context, this study contributed to the IA implementation and eGovernment literature. This work will serve as a basis for researchers to develop more precise IA implementation models for eGovernment. Finally, the findings of this study will assist policymakers in the IA implementation for Indonesian eGovernment initiatives to set a strong foundation for successful IA implementation.

Table 5.9 The confirmed framework

Category		Factors
Organisational Management	1	Leadership and Commitment
	2	Policy, Legal, and Compliance
	3	Management Review and Continual Improvement
	4	Holistic Approach
	5	Business Alignment
	6	Organisational Roles, Responsibilities, and Authorities
	7	Awareness, Education, and Training
Implementation Management	1	Risk Management
	2	Security Objectives
	3	Operations and Management
	4	Performance Evaluation
	5	Recovery and Continuity Management
	6	Infrastructures Development
Social Management	1	Cultural Issues
	2	Digital Divide
	3	Trust and Privacy
	4	Organisational Structures
	5	Coordination

5.4 Summary

This chapter confirmed the identified factors affecting the implementation of IA for eGovernment in Indonesia. From the findings, it was acknowledged that all the identified factors indicated as important by the experts regarding the IA implementation for e-Government in Indonesia. Moreover, the results from the survey that was distributed to IA, e-Government, information security practitioners in Indonesia, indicated that all factors are statistically significant.

Chapter 6 The development and validation of the instrument

After analysing the findings and results of the experts' reviews, and practitioners survey; the framework was refactored, analysed, and adjusted (see Chapter 5). Although it has combined groups of factors that are considered important on both global and cultural level, specifically in terms of the successful implementation of IA, the framework requires further developments to create a more practical form that can be tested in the involved organisations. The most direct option is to implement the framework is to develop an instrument and use it for assessing the success of IA implementation. Moreover, to ensure that the framework is applicable for eGovernment in Indonesia, it should be examined in the same context. Consequently, the instrument should be tested in different public organisations in Indonesia.

The validation of the instrument went through many phases, from developing the instrument and preparing the case studies to conduct the studies and receiving the participants' evaluation. To evaluate the IA instrument and procure the most accurate feedback, case studies were carried out on three public organisations in Indonesia. The participants of the case studies were asked to share their opinion on the usability and quality of the instrument and to describe the extent to which the results reflected the reality of the organisation. In turn, these quantitative and qualitative studies were used to validate the instrument. As requested by the university, the studies were built on the respondents' anonymity. The Ethics Form ERGO/FOPSE/41817 was completed, and all respondents were asked to read and agree to a consent form before participating in the study.

6.1 Developing the instrument

The confirmed framework will be developed for use as a research instrument to measure IA implementation process within organisations in Indonesia. The instrument will be developed based on the Goals Question Metric (GQM) approach. The GQM approach is chosen since it defines a measurement model that aids in answering a variety of questions associated with the performance of a process. It helps to determine the strengths and weaknesses of the current processes, and it provides a rationale for adopting/refining techniques, to evaluate the quality and impact of a specific process. Therefore, developing an instrument based on this approach helps to measure the IA implementation process in an organisation by answering questions associated with the performance of each practice.

Accordingly, the development of the instrument starts with the goal of achieving the factors that need to be measured. Each factor is then refined into instrumental questions and then each question is refined into metric.

In this instrument, the Goals are the factor items from the IA framework. Moreover, the Questions in this instrument are the Instrumental Questions which represent the components of each factor and act as the basic parameters of the level of IA status within an organisation. Lastly, the Metric in the instrument is a scale developed for the organisation to be able to answer the Instrumental Questions for assessing its IA level.

The category of Organisational Management (OM) has seven Goals on the instrument that must be measured. These seven Goals are based on seven factors from the OM category. Each of these Goals forms the basis for generating Questions or in this instrument called Instrumental Questions. Instrumental Questions function as questions to measure characteristics that must be met to achieve Goals.

The instrument questions came from the initial purpose of the instrument. These questions were developed by the author based on the framework and had been pre-tested (see section 6.2) before being used in the case studies. Each question in the instrument is expected to be able to measure the status of each factor. For example, the Leadership and Commitment factor has two Instrumental Questions. This is intended to address two characteristics that must be met in achieving this factor. Both Instrumental Questions address questions for Leadership and Commitment in an organisation and the answer will be used as the basis for measuring the status of the factor. The overall Goals and Instrumental Questions for OM categories can be seen in Table 6.1.

Table 6.1 IA measurement instrument for Organisational Management

Cat No	**Category Items**	**Factor No**	**Factor Items**	**Instrumental Questions**
1	Organisational Management (OM)	1	Leadership and Commitment	The lead of board of directors to IA implementation?
				The commitment of board of directors to IA implementation?
		2	Policy, Legal, and Compliance	The availability of policy to provide management direction and support for IA in accordance with business requirements?
				The availability of legal aspects to identify the organisation's legal

				obligation (statutory, regulatory, and contractual)?
				The availability of appropriate procedures to ensure compliance with the legal aspects that apply to the organisation?
		3	Management Review and Continual Improvement	The periodic review (regarding the suitability, adequacy, and effectiveness) of the information assurance policy by senior management?
				The continual improvement of the information assurance policy by senior management?
		4	Holistic Approach	The treatment of IA as a combination of the physical, procedural, personnel, and technical security?
		5	Business Alignment	The alignment between IA implementation and the organisation's business needs?
		6	Organisational Roles, Responsibilities, and Authorities	The senior management assigned and communicated organisational roles relevant to IA?
				The senior management assigned responsibilities for ensuring IA is in accordance with the policy?
				The senior management assigned authorities to confirm information assurance is in accordance with the policy?
		7	Awareness, Education, and Training	The awareness of all employees in the organisation on their contribution to the IA implementation?
				The education of all employees in the organisation as relevant for their job function?
				The training of all employees in the organisation as relevant for their job function?

Secondly, for the Implementation Management (IM) category, there are six Goals on the instrument that must be measured based on six factors from the IM category. Each Goal has a varied number of questions. This depends on the number of characteristics that must be met in achieving these factors.

Operations and Management factor has the most Instrumental Questions, namely three questions. These three questions are needed to address the characteristics that must be met, namely on the aspects of the plan, implementation, and control. All Goals and Instrumental Questions for the IM category can be seen in Table 6.2.

Table 6.2 IA measurement instrument for Implementation Management

Cat No	**Category Items**	**Factor No**	**Factor Items**	**Instrumental Questions**
2	Implementation Management (IM)	1	Risk Management	The adopted of risk management strategy of IA implementation?
		2	Security Objectives	The relevance of information security objectives to the functions and levels.
		3	Operations and Management	The plan of information security complied with information security policy?
				The implementation of information security complied with information security policy?
				The control of information security complied with information security policy?
		4	Performance Evaluation	The performance evaluation (relating to the effectiveness and maintenance) of the IA implementation?
		5	Recovery and Continuity Management	The adopted of disaster recovery plan of IA implementation?
				The adopted of business continuity plan in the event major failures?
		6	Infrastructure Development	The required relevant technology and infrastructure of IA implementation?

Lastly, the Social Management (SM) category has five Goals on the instrument that must be measured based on five factors from the SM category. Just like the previous categories, each Goal has a variety of questions. The characteristics that must be met in achieving these factors are considered the number of questions.

Trust and Privacy factors have the most Instrumental Questions, namely two questions. Both questions address characteristics that must be fulfilled, namely the aspects of trust and privacy. The overall Goals and Instrumental Questions for the IM category can be seen in Table 6.3.

Table 6.3 IA measurement instrument for Social Management

Cat No	Category Items	Factor No	Factor Items	Instrumental Questions
3	Social Management (SM)	1	Cultural Issues	The consideration of cultural issues in the organisation during the implementation of IA?
		2	Digital Divide	The consideration of digital literacy issue in the organisation during the implementation of IA?
		3	Trust and Privacy	The established of trust between government and citizens?
				The protection regarding privacy of information?
		4	Organisational Structures	The creation of a division to be in control of handling information security issues?
		5	Coordination	The coordination between institutions regarding the duties of each institution?

The approach results in a specification of a measurement system targeting a set of rules for the interpretation of the measurement data in a top-down hierarchical structure. The structure includes the conceptual level (Goals) which is the object of measurement, then the operational level (Questions) that characterises the way the achievement of the goal is going to be performed, followed by the quantitative level (Metric) which is the data associated with every question to be answered quantitatively.

A metric of six scales for the instrument adapted from the COBIT 5 Process Assessment Model which is based on ISO/IEC 15504-2:2003 will be used to measure the IA implementation process as follows:

- Level 0: Incomplete process
- Level 1: Performed process
- Level 2: Managed process
- Level 3: Established process
- Level 4: Predictable process
- Level 5: Optimising process

However, after conducted pre-test with five experts (see section 6.2), participants described that the naming of Incomplete process, Performed process, and Predictable process were not very clear and difficult to understand. Therefore, the scale was defined and re-ordered by adding Non-existent process, Initial process, and Optimised process. Then, to enhance the readability of the answers, each answer was given an equivalent percentage that indicates the success status of that factor. It's clear that "Non-existent" equals zero and "Optimised" represents 100%, which makes the parameters between 20%, 40%, 60%, and 80% when 100% is divided by 5.

So, the metric used in the instrument are as follows:

- Level 0: Non-existent process = 0%
- Level 1: Initial process = 20%
- Level 2: Defined process = 40%
- Level 3: Managed process = 60%
- Level 4: Established process = 80%
- Level 5: Optimised process = 100%

To make the results more informative, and to offer recommendations to the organisations, the indication of the results will be shown as follows:

- Level 0 – Non-existent Process: The process is not adopted or implemented.
  This indicates the presence of "Severe Areas, and serious and critical action is needed".
- Level 1 – Initial Process: The process is not implemented properly and/or fails to achieve its purpose. Consequently, the process is informal and uncoordinated.
  Which indicates that there are "Below-Average Areas and major and urgent action is needed".
- Level 2 – Defined Process: The process is implemented, documented, and communicated simply; it achieves its process purpose.
  Which indicates that those areas are "Moderate Areas and medium improvement is needed".
- Level 3 – Managed Process: The defined process is now implemented in a managed fashion (planned, monitored, and adjusted).
  Which indicates that those areas are "Above-Average Areas and minor improvement is needed".
- Level 4 – Established Process: The managed process is now implemented using a defined process that is capable of achieving its process outcomes and its work products are appropriately measured, controlled and maintained.

Which indicates that those areas are “Solid Areas and minor improvement may be needed”.

- Level 5 – Optimised Process: The established process is continuously improved, and best practices are followed to meet current and projected business goals.
  Which indicates that those areas are “Perfect Areas and no action is needed”.

These indications of the results were adapted from COBIT 5 Process Assessment Model and were modified to fit for assessing IA status in the Indonesian context. The results were discussed with the experts and agreed upon in the pre-test phase. In addition, participants are asked about the status of each factor in their organisation and to choose one measure as an answer. All questions began as follows: “What do you think is the status of...”

6.2 Pre-test

Pre-test research was conducted to shape the instrument appropriately before carrying out case studies. The research was pre-tested with five experts, three from Indonesian government agencies and two are academic researchers, for identifying problems in the language, tone, structure and design of a questionnaire that is used for the case studies. First, participants were contacted to take part in the study. After they accepted to get involved in the study, the instrument subsequently was sent to five IA and eGovernment specialists. Then, interviews were conducted to explain the research and the instrument itself. They provided good recommendations. Although they were pleased with the instrument, they suggested some modifications. First, they suggested changing “Incomplete process”, “Performed process”, and “Predictable process” from the answer metric into more clear responses and also the suggested to re-ordering the metric; they mentioned that these responses were unclear and difficult to understand. Moreover, they suggested adding percentages equivalent to the metric numbers, as shown in section 6.1. Ultimately, the instrument was deemed ready to be used in the main case studies. For the final score, a scale was proposed similar to the results’ indication of the categories’ final score (as shown in the previous section), and by following the COBIT 5 Process Assessment Model (PAM) and ISO/IEC 15504-5:2012 metric indications. The experts agreed on the scale and all parties involved reached a consensus regarding the scoring process. The scale is shown as following:

- Any score from 0% to 12%: **Level 0 Status -** serious and critical improvements are needed.
- Any score from 12.50% to 37%: **Level 1 Status -** Major and urgent improvements are needed.
- Any score from 37.50% to 50%: **Level 2 Status -** Medium improvements are needed.
- Any score from 50.50% to 62%: **Level 3 Status -** Minor improvements are needed.
- Any score from 62.50% to 87%: **Level 4 Status -** Minor improvements may be needed.
- Any score from 87.50% to 100%: **Level 5 Status -** No action is needed.

6.2.1 Calculating the final scores

The developed scale was used in the final scores. Two calculations were completed after determining the scores of the factors (the category scores before weighting) and the whole IA score. These will be explained in the following sections.

6.2.1.1 Calculating the category scores before weighting

After determining the score of each factor, the score of each category was calculated before weighting that category within the whole framework. This was done by collecting the scores of the factors (F) in each category and dividing the total by the number of factors in that category:
Organisational Management (OM) weight = (F1 score +…+ F7 score) / No. of factors (7)
Implementation Management (IM) weight: (F1 score + … + F6 score) / No. of factors (6)
Social Management (SM) weight: (F1 score + F2 score + F5 score) / No. of factors (5)

- Any score from 0% to 12%: **Level 0 Status**.
- Any score from 12.50% to 37%: **Level 1 Status**.
- Any score from 37.50% to 50%: **Level 2 Status**.
- Any score from 50.50% to 62%: **Level 3 Status**.
- Any score from 62.50% to 87%: **Level 4 Status**.
- Any score from 87.50% to 100%: **Level 5 Status**.

6.2.1.2 Calculating the whole IA score

After determining the scores of the categories within each organisation, simple calculations were carried out to identify the final weight of IA (again, for each organisation). In doing so, the following steps were taken:

1. First, the weight of each factor was calculated. This was done by dividing 100 by the No. of factors in all categories:
   The factor weight = 100/ (No. of the factors in all categories: 7+6+5) = 100/18 = **5.56**

2. Then, the full weight of each category was calculated:

   Full Category weight = Factor weight (5.56) * No. of factors in each category.

   Full Organisational Management (OM) weight = 5.56 * No. of factors (7) = **38.9%**

   Full Implementation Management (IM) weight = 5.56 * No. of factors (6) = **33.3%**

   Full Social Management (SM) weight = 5.56 * No. of factors (5) = **27.8%**

3. After that, the weight of each category in the organisation was calculated. This consisted of multiplying the full category weight by the final score of that category, and then dividing that figure by 100, for example:

   OM weight in organization X = Category Weight (38.9) * OM final score in Organization X

4. Finally, the total score of the IA in Organization X is the total of all categories' weight in the organisation:

   IA Final Score in Organisation X = OM weight in organisation X + IM weight in organisation X + SM weight in organisation X

6.3 Case studies

After obtaining and analysing the results of the pre-test, qualitative and quantitative studies were conducted using the instrument. The instrument was examined in government offices in Indonesia that have fully or partially implemented eGovernment services and IA. Comprehensive case studies of three organisations were carried out using the instrument, with the purpose of measuring the extent to which these organisations' implementation of IA for eGovernment has proven successful. Permission was obtained from all three organisations in advance, at which point a substantial effort was made to prepare for the study with the participants. Subsequently, the instrument was prepared and developed as a questionnaire. Then, the case studies were carried out. After obtaining and analysing the results of these case studies, quantitative and qualitative studies were conducted to complete the validation of the instrument.

6.3.1 Getting permission

The instrument was examined in Indonesia, in governance office that has fully or partially implemented IA and eGovernment. Consequently, a sound effort was made to identify organisations that met those requirements, and that were willing to participate in the case study. This process began before and continued after the pilot took place. The following organisations participated in the case studies are one public sector organisation, one local government, and one provincial government.

Correspondingly, before conducting the main study, permission was requested of these organisations, at which point the communication started with either their governance office, IT management or top management. The bureaucracy system of public organisations in Indonesia made gaining permission a difficult and lengthy process. That said, by forging a connection with the key employees in each organisation, the three case studies were able to begin in a timely manner. A substantial effort was made to reach executives in governance, IT and other departments in order to begin the study. Unofficial meetings, messaging and phone calls were the main channels we used to contact these people. The permission was granted immediately after the first communication. Because of the confidentiality agreement between the researcher and the organisations, the differences between the participating organisations and their response processes cannot be revealed.

6.3.2 Developing the case study tool

As explained in the methodology chapter, the only possible way of gathering the necessary data from the three organisations was to get one accurate assessment of IA. This was undertaken by the focus group, which was the best option given the circumstances. The main target of the focus group was to provide a single completed questionnaire on behalf of the organisation in question.

To ensure a clear and accurate assessment of the targeted organisations' status, a structured questionnaire was used to gather their responses. The questionnaire featured a general explanation of the rating scales or the following six assessment levels:

- Level 0 – Non-existent Process: The process is not adopted or implemented.
  This means it's a Severe Factor and its score is 0%.
- Level 1 – Initial Process: The process is not implemented properly and/or fails to achieve its purpose. Consequently, the process is informal and uncoordinated. This means it is a Below-Average Factor and its score is 20%.
- Level 2 – Defined Process: The process is implemented, documented, and communicated simply; it achieves its process purpose. This means it is a Moderate Factor and its score is 40%.
- Level 3 – Managed Process: The defined process is now implemented in a managed fashion (planned, monitored, and adjusted). This means it is an Above-Average Factor and its score is 60%.
- Level 4 – Established Process: The managed process is now implemented using a defined process that is capable of achieving its process outcomes and its work products are

appropriately measured, controlled and maintained. This means it is a Solid Factor and its score is 80%.

- Level 5 – Optimised Process: The established process is continuously improved, and best practices are followed to meet current and projected business goals. This means it is a Perfect Factor and its score is 100%.

Next, the focus group participants were interviewed to provide a clear view of the study. The sample consisted of 9 to 10 participants from different levels and departments (executives, governance officers, IT managers, etc.).

Finally, the focus group interview was conducted in each organisation to record an accurate answer for all factors. This method allowed participants to feel much more comfortable about the confidential nature of the study, and thus, they answered the questionnaire accurately.

Next, the weighting of the categories and factors took place, and scores were calculated for each factor, category and the full framework. The results are shown in the radar charts (see Chapter 7).

6.3.3 Case study installation

A case study may be literally replicated, when the case is selected to predict similar results, or it is theoretically replicated, when the case is selected to predict contrasting results for predictable reasons (Yin, 2003). This study will conduct literally replicated, since the developed instrument is for government organisations. Therefore, the case study conducted in public sector to predict similar results from the public sector. The case studies analysed the status of IA implementation for eGovernment in each organisation and the respondents' feedback regarding the instrument.

The instrument was applied in three case studies. Due to the confidentiality agreement, the results were assigned to the case study number rather than to the name of the organisation. After conducting the focus group sessions and procuring the questionnaire results, the assessment of IA in the participating organisations took place.

As in the framework and the questionnaire, this study covered three main categories of IA (Organisation Management, Implementation Management, Social Management), and under each category were factors represented by the questions. In this chapter, the assessment of the factors in each category were presented first, followed by the assessment of the main categories. Each organisation filled out one questionnaire and provided a single accurate answer for each question.

The assessment results were displayed in radar charts and are presented in the main report. Then, a brief translation of the charts and numbers will be presented, at which point feedback on each

question was presented as well. Finally, the participants' opinions of the whole instrument were documented.

6.3.3.1 Case study description and structure

In the first stage of each case study, participants were asked to choose the status for each question. Then, in the second stage, the results file was submitted and discussed with the main participants. The file contains radar and bar charts, and it shows the scores of the factors in each category.

After each category, participants were asked, **"To what extent do you agree that these results reflect the actual status of 'Category X' in your organisation?"** In addition, another radar chart was presented, showing the scores of all categories. At the end of that file, the final score of IA in the organisation was presented. Following the final score, the participants were asked two questions: **"To what extent do you agree that these results reflect the actual status of IA in your organisation?"** and **"To what extent do you agree that this instrument is a good instrument for measuring IA implementation process for eGovernment in Indonesia?"** The assessment results report was shown to the participants was explained clearly too.

In the case studies chapter, each case study covered the organisation, the results of the case study, the analysis and discussion of the study, and ultimately, a summary. The results section presented a table summarising the results of all case study components, including the factor scores, category scores, whole IA score and the participants' responses to all questions. This table refers to the instrument, adding the scores of the categories, factors and the whole IA.

In the analysis section, the radar charts of the categories were depicted exactly as shown for the participants, with brief interpretations of the charts included. The feedback analysis of all questions was shown afterwards. The implications of the results and the analysis will be shown in the last section of the chapter, the discussion section.

6.4 Summary

The instrument was developed by using the confirmed information assurance framework as a reference. The Goals Questions Metric (GQM) approach was followed In order to develop this instrument. Each component contained several questions and a metric of six scales adapted from COBIT 5 Process Assessment Model which is based on ISO/IEC 15504-2:2003 was used to measure the IA implementation process. The answers then were weighted and added up to a total score.

The instrument was pre-tested before it was used. Interviews involved five experts were conducted to complete the pre-test. There are some comments made by the experts regarding the instrument.

It was suggested to change some scale names to be clearer and to avoid confusion. Moreover, the experts also suggested adding a percentage on every scale to give more clearance and to help during the assessment process. Lastly, all experts also agreed on the proposed final score scales which was adapted from the COBIT 5 Process Assessment Model (PAM) and ISO/IEC 15504-5:2012.

Chapter 7 Findings, results, and discussions of the case studies

This chapter presents the results and discusses the case studies conducted using the instrument developed based on the IA framework (see Section 6.1). After the instrument had been piloted and confirmed, it was then validated by conducting case studies. The case studies were intended to assess the IA implementation in Indonesian government institutions as a process to validate the effectiveness and feasibility of the instrument that has been developed. The case studies were conducted in three government institutions in Indonesia. The institutions had been implemented eGovernment services with a varied time period. The summary at the end of the chapter presents the conclusions derived from the case studies results.

7.1 The first case study

The first case study was conducted in one of the public sectors in Indonesia with over 28,000 employees. There were 10 participants involved. One participant was from senior management, three IT management, and six IT staff. The organisation was established with the current structure in 1995, while the eGovernment services have been implemented since 2014. The results of the study in this organisation are shown below.

7.1.1 The results of the first case study

In this section, the results of the first case study are shown. Table 7.1 presents the results for the Organisational Management (OM) category.

Table 7.1 The results of the first case study for OM

Cat No	Category Items	Factor No	Factor Items	Instrumental Questions	Scores
1	Organisational Management (OM) Score: 42.38% Response: Strongly Agree	1	Leadership and Commitment	The lead of board of directors to IA implementation?	40%
				The commitment of board of directors to IA implementation?	40%
		2	Policy, Legal, and Compliance	The availability of policy to provide management direction and support for IA in accordance with business requirements?	40%
				The availability of legal aspects to identify the organisation's legal obligation (statutory, regulatory, and contractual)?	40%
				The availability of appropriate procedures to ensure compliance with the legal aspects that apply to the organisation?	40%
		3	Management Review and Continual Improvement	The periodic review (regarding the suitability, adequacy, and effectiveness) of the information assurance policy by senior management?	20%
				The continual improvement of the information assurance policy by senior management?	40%
		4	Holistic Approach	The treatment of IA as a combination of the physical, procedural, personnel, and technical security?	60%
		5	Business Alignment	The alignment between IA implementation and the organisation's business needs?	40%
		6	Organisational Roles, Responsibilities, and Authorities	The senior management assigned and communicated organisational roles relevant to IA?	60%
				The senior management assigned responsibilities for ensuring IA is in accordance with the policy?	60%
				The senior management assigned authorities to confirm	20%

				information assurance is in accordance with the policy?	
		7	Awareness, Education, and Training	The awareness of all employees in the organisation on their contribution to the IA implementation?	40%
				The education of all employees in the organisation as relevant for their job function?	40%
				The training of all employees in the organisation as relevant for their job function?	40%

The score of OM category is 42.38%. This score is obtained from the calculation of the scores of the Instrumental Questions, which have 15 questions. These scores are the result of measurements for seven factor items in the OM category. Further, the participants stated they strongly agreed to the results of the OM category for their organisation. Moreover, Table 7.2 presents the results of the first case study for the Implementation Management category.

Table 7.2 The results of the first case study for IM

Cat No	**Category Items**	**Factor No**	**Factor Items**	**Instrumental Questions**	**Scores**
2	Implementation Management (IM) Score: 38.89% Response: Agree	1	Risk Management	The adopted of risk management strategy of IA implementation?	40%
		2	Security Objectives	The relevance of information security objectives to the functions and levels.	40%
		3	Operations and Management	The plan of information security complied with information security policy?	40%
				The implementation of information security complied with information security policy?	40%
				The control of information security complied with information security policy?	20%
		4	Performance Evaluation	The performance evaluation (relating to the effectiveness and maintenance) of the IA implementation?	20%
		5		The adopted of disaster recovery plan of IA implementation?	40%

			Recovery and Continuity Management	The adopted of business continuity plan in the event major failures?	40%
		6	Infrastructure Development	The required relevant technology and infrastructure of IA implementation?	60%

The IM category has nine Instrumental Questions for measuring six Factor Items. The result of the calculation from the nine Instrument Questions scores is 38.89%. Moreover, participants agreed that this score represented the IM status in their organisation. Lastly, the results for Social Management (SM) category are presented in Table 7.3 below.

Table 7.3 The results of the first case study for SM

Cat No	Category Items	Factor No	Factor Items	Instrumental Questions	Scores
3	Social Management (SM) Score: 44% Response: Strongly Agree	1	Cultural Issues	The consideration of cultural issues in the organisation during the implementation of IA?	40%
		2	Digital Divide	The consideration of digital literacy issue in the organisation during the implementation of IA?	20%
		3	Trust and Privacy	The established of trust between government and citizens?	60%
				The protection regarding privacy of information?	60%
		4	Organisational Structures	The creation of a division to be in control of handling information security issues?	60%
		5	Coordination	The coordination between institutions regarding the duties of each institution?	40%

The score for the SM category is 44%. This score is the result of calculating scores from six Instrumental Questions for measuring five Factor Items. Furthermore, the participants strongly agreed that this score represented the status of SM in their organisation.

7.1.2 The analysis of the first case study

This section presents factor analysis, categories analysis and feedback analysis from the first case study.

7.1.2.1 Factors analysis

The factor analysis of the first case study is presented in Table 7.4 as shown below. The table presents the status of each of the factors obtained from the case study conducted.

Table 7.4 The factors analysis of the first case study

Factor Category	Factor Name	Factor Status
OM	Holistic Approach	Level 3 (60%)
IM	Infrastructure Development	
OM	Organisational Roles, Responsibilities, and Authorities	Between Level 2 and Level 3 (40%-60%)
OM	Leadership and Commitment	Level 2 (40%)
	Policy, Legal, and Compliance	
	Business Alignment	
	Awareness, Education, and Training	
IM	Risk Management	
	Security Objectives	
	Recovery and Continuity Management	
SM	Cultural Issues	
	Coordination	
OM	Management Review and Continual Improvement	Between Level 1 and Level 2 (20%-40%)
IM	Operations and Management	
IM	Performance Evaluation	Level 1 (20%)
SM	Digital Divide	

7.1.2.2 The categories analysis of the first case study

The analysis of the categories from the first case study are presented with radar chart as shown in Figure 7.1. The radar chart presents the results of weight calculations from each category. In addition to that, a recommendation is given based on results.

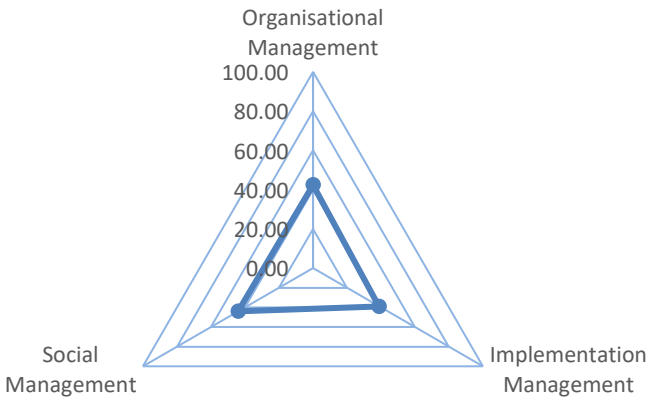

Figure 7.1 The radar chart of the first case study

The results from the categories analysis are defined below:

Level 2 categories:

1. **42.38%,** Organisational Management
2. **38.89%**, Implementation Management
3. **44%,** Social Management

The calculation can be found in Appendix G. Case Studies Calculation

7.1.2.3 Feedback analysis

Table 7.5 presents the analysis of the feedback of the participants from the first case study. In addition, this sub-section presents the participants' comments about the first case study.

Table 7.5 The feedback analysis of the first case study

Questions	Responses
Q1. Organisational Management, 42.38% Q3. Social Management, 44% Q4. Whole IA is Level 2 status, 41.67% Q5. Good Instrument	Strongly Agree
Q2. Implementation Management, 38.89%	Agree

With the score of 42.38% for the Organisational Management category, the participants strongly agreed that the score represented the OM category of the IA implementation status in their organisation. Further, participants commented that Leadership and commitment from leaders in their organisation are good, so that the implementation of projects in organisations, e.g. IA will always be guaranteed to be continued even though there is a change of leadership. However, despite the leadership and commitment are good, there is no policy for periodic review. Usually, reviews are carried out in an incidental manner, such as if there is an event or an audit is carried

out and then from the results, improvement will be made. Nevertheless, for training, staff are more self-taught, because training is not given regularly, but if there is a request, it will be given.

For the second category, which is Implementation Management, participants agreed with the score. It means the score of 38.89% represents the status of their IA implementation for the category in their organisation. Moreover, they mentioned that for the security objectives aspect, there are already functions dedicated to physical, procedural, personnel, and technical, and also everything is well-monitored. Further, staff competency on the functions of their job within the organisation is good. Performance evaluations such as audits, monitoring, etc. on IA implementation have not been conducted regularly.

The score for the Social Management category in their organisation is 44%. They also strongly agreed that this score represented the status of the IA implementation in their organisation. They also remarked that for the problems of culture and habits of Indonesians, especially in the organisation, there are procedures and policies to deal with them. This has been communicated to each staff member but in its implementation, it has not been well monitored. In addition, the issue of the digital divide in this organisation has not been handled properly. For example, there are still employees who are placed in the IT division but do not understand IT. And as previously stated, no planned training, unless requested.

The final score of the status of IA implementation in their organisation is 41.67%, which means their organisation has Level 2 status for the implementation. They expressed their satisfaction with the results and also agreed that the results represented their organisation IA status. Moreover, there are some comments regarding the instrument itself. The participant stated that the use of instruments is not difficult, and the scale is easy to understand. They also answered during afterthought session that the instrument is a good instrument for measuring IA. Lastly, they are interested if there is an update on this study.

7.1.3 The discussion of the first case study

It is clear from the results that the categories are average, with factors that vary from Level 1 to Level 3. The results are obtained because the scores of the factors at each level affect the final score of the category. For example, the Social Management category has two factors in the Level 3 category but has two factors in the Level 2 category, and one factor in the Level 1 category so that the final score is Level 2 category.

Likewise, the whole IA implementation scored Level 2 status. This means the number and the scores of categories at each level affect the overall score of the implementation. In this case study, the results are three Level 2 categories, hence the final score is Level 2.

It can be seen that in this organisation, the participants have strongly agreed on the assessment of most categories, and they agreed that the final score reflected the true success (or lack thereof) of the IA implementation in their organisation thus. In addition, they expressed that the instrument is a good instrument when it comes to measuring IA in the Indonesia government organisations. They seem pleased with all components of the instrument and would complete the assessment again.

7.2 The second case study

This organisation is one of the provincial government organisations in Indonesia. There are over 72,000 employees working under this organisation. There were 10 participants involved. One participant was from senior management, two IT management, and seven IT staff. They have implemented eGovernment since 2008. The results of the study in this organisation are shown below.

7.2.1 The results of the second case study

The results of the case second case study are presented in this section. Table 7.6 shows the results for the Organisational Management (OM) category.

Table 7.6 The results of the second case study for OM

Cat No	Category Items	Factor No	Factor Items	Instrumental Questions	Scores
1	Organisational Management (OM) Score: 29.52% Response: Agree	1	Leadership and Commitment	The lead of board of directors to IA implementation?	20%
				The commitment of board of directors to IA implementation?	20%
		2	Policy, Legal, and Compliance	The availability of policy to provide management direction and support for IA in accordance with business requirements?	40%
				The availability of legal aspects to identify the organisation's legal obligation	40%

				(statutory, regulatory, and contractual)?	
				The availability of appropriate procedures to ensure compliance with the legal aspects that apply to the organisation?	20%
		3	Management Review and Continual Improvement	The periodic review (regarding the suitability, adequacy, and effectiveness) of the information assurance policy by senior management?	20%
				The continual improvement of the information assurance policy by senior management?	20%
		4	Holistic Approach	The treatment of IA as a combination of the physical, procedural, personnel, and technical security?	20%
		5	Business Alignment	The alignment between IA implementation and the organisation's business needs?	20%
		6	Organisational Roles, Responsibilities, and Authorities	The senior management assigned and communicated organisational roles relevant to IA?	40%
				The senior management assigned responsibilities for ensuring IA is in accordance with the policy?	40%
				The senior management assigned authorities to confirm information assurance is in accordance with the policy?	20%
		7	Awareness, Education, and Training	The awareness of all employees in the organisation on their contribution to the IA implementation?	20%
				The education of all employees in the organisation as relevant for their job function?	80%

				The training of all employees in the organisation as relevant for their job function?	80%

The score for the OM category in the second case study was 29.52%. This score represents the calculation result of the total scores obtained by answering 15 Instrumental Questions. The participants agreed that this score represented the OM status for IA implementation in their organisation. Yet, Table 7.7 presents the results for Implementation Management (IM) category.

Table 7.7 The results of the second case study for IM

Cat No	Category Items	Factor No	Factor Items	Instrumental Questions	Scores
2	Implementation Management (IM) Score: 41.11% Response: Strongly Agree	1	Risk Management	The adopted of risk management strategy of IA implementation?	60%
		2	Security Objectives	The relevance of information security objectives to the functions and levels.	40%
		3	Operations and Management	The plan of information security complied with information security policy?	40%
				The implementation of information security complied with information security policy?	20%
				The control of information security complied with information security policy?	20%
		4	Performance Evaluation	The performance evaluation (relating to the effectiveness and maintenance) of the IA implementation?	20%
		5	Recovery and Continuity Management	The adopted of disaster recovery plan of IA implementation?	20%
				The adopted of business continuity plan in the event major failures?	20%
		6	Infrastructure Development	The required relevant technology and infrastructure of IA implementation?	80%

From the calculation of the scores, which are the results of answering nine Instrumental Questions for the measurement of Factor Items, for the IM category a score of 41.11% was obtained. This

score represents the IM status of their organisation in implementing IA and the participants strongly agree with this score. Further, Table 7.8 presents the results for the Social Management (SM) category.

Table 7.8 The results of the second case study for SM

Cat No	Category Items	Factor No	Factor Items	Instrumental Questions	Scores
3	Social Management (SM) Score: 32% Response: Strongly Agree	1	Cultural Issues	The consideration of cultural issues in the organisation during the implementation of IA?	20%
		2	Digital Divide	The consideration of digital literacy issue in the organisation during the implementation of IA?	20%
		3	Trust and Privacy	The established of trust between government and citizens?	40%
				The protection regarding privacy of information?	80%
		4	Organisational Structures	The creation of a division to be in control of handling information security issues?	20%
		5	Coordination	The coordination between institutions regarding the duties of each institution?	40%

The SM category for the second case study, after calculating the scores from six Instrumental Questions, scored 32%. The participants strongly agreed to this score. Which means that this score represents the status of SM in the implementation of IA in their organisation.

7.2.2 The analysis of the second case study

Analyses of the results of the second case study are presented in this section, including factor analysis, categories analysis, and feedback analysis.

7.2.2.1 Factors analysis

The results of factor analysis from the second case study are presented as shown in Table 7.9.

Table 7.9 The factors analysis of the second case study

Factor Category	Factor Name	Factor Status
IM	Infrastructure Development	Level 4 (80%)
OM	Awareness, Education, and Training	Level 3 (60%)
IM	Risk Management	
SM	Trust and Privacy	
IM	Security Objectives	Level 2 (40%)
SM	Coordination	
OM	Policy, Legal, and Compliance	Between Level 1 and Level 2 (20%-40%)
	Organisational Roles, Responsibilities, and Authorities	
IM	Operations and Management	
OM	Leadership and Commitment	Level 1 (20%)
	Management Review and Continual Improvement	
	Holistic Approach	
	Business Alignment	
IM	Performance Evaluation	
	Recovery and Continuity Management	
SM	Cultural Issues	
	Digital Divide	
	Organisational Structures	

7.2.2.2 The categories analysis of the second case study

Figure 7.2 shows the radar chart of the categories' analysis of the second case study. Besides, a recommendation action is also suggested based on the results.

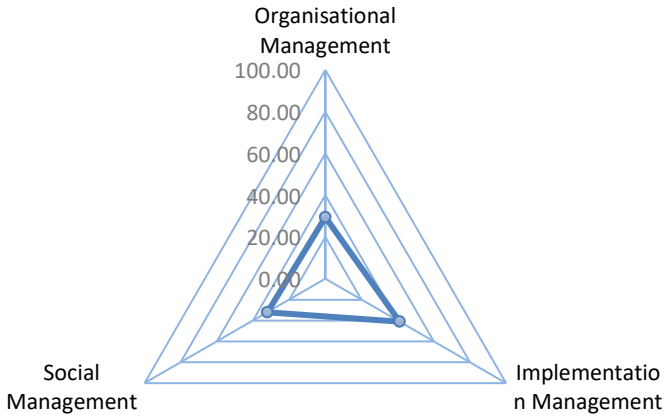

Figure 7.2 The radar chart of the second case study

Level 2 categories:

1. **41.11%**, Implementation Management

Level 1 categories:

1. **29.52%,** Organisational Management
2. **32%,** Social Management

The calculation can be found in Appendix G. Case Studies Calculation

7.2.2.3 Feedback analysis

The afterthought feedback of the second case study from participants are presented in Table 7.10 and the comments presented as follows.

Table 7.10 The feedback analysis of the second case study

Questions	Responses
Q2. Implementation Management, 41.11% Q3. Social Management, 32% Q5. Good Instrument	Strongly Agree
Q1. Organisational Management, 29.52% Q4. Whole IA is Level 1 status, 34.07%	Agree

The score of OM for this organisation is 29.52%. This low score is agreed on by participants. Moreover, according to participant comments, there are some issues in their organisation that resulting in this low score. Such issue as, the highest leader in the organisation does not have qualified knowledge of IA, in addition to the lack of commitment. This resulted in a lack of actions to support the implementation of IA properly. Also, despite the existing of policy and legal, it has not yet been made a binding procedure or regulation to comply with the existing policy and legal. Further, usually review is carried out using SCRUM or TRELLO. But the review has not yet followed to a certain standard. More, IA has not been projected to support the business needs of the organisation. The organisation here has not included IA aspect when planning business plans, so IA is still focusing on things like password security and websites. Further, in this organisation people who are appointed to be responsible for some roles are sometimes incompetent and not suitable for the positions.

Next, participants strongly agreed that the score of 41.11% represented their organisation IM status in the IA implementation. They remarked that factor items in this category already exist and supports the business, but, has not been completely integrated to be in line with the business. They also stated that the adoption of risk management starting from planning, monitoring, and

adjustments have been done even though it has not used a certain standard. Then, the technical implementation of security has been carried out, but the main problem is more on the human aspect. For example, many staff still use their default password for their account. Yet, performance evaluation has not been done regularly. More, continuity management is also not yet standardised even though they already have the continuity plan. Despite these issues, the infrastructure in this organisation is very good because it is an organisation that has a large budget for infrastructure expenditure.

Further, participants also strongly agreed that the SM category with a score of 32% represented their SM status. They made some comments regarding this category, such as there is still frequent resistance to change and openness from a large number of staffs. In addition, digital illiteracy is still common in this organisation due to the incompatibility of the staff background with their job. For the coordination factor, because there are still many unclear regulations regarding the roles for staff and lack of coordination in work, sometimes they have to do things that are not their responsibility and overlap with other staff work.

At last, participants agreed with the final score. The final score is 34.07%, which means, whole IA implementation is on the Level 1 status. They also responded in the afterthought session with strongly agree response if this instrument is a good instrument and expressed that the measurement results reflect IA's status in this organisation and provide awareness about IA's condition in this organisation. In conjunction with that, they suggested that it would be better if there is a list of processes or levels to help to decide a score from the metric during the assessment process.

7.2.3 The discussion of the second case study

Based on the results, it is clear that the IA status in the organisation is Level 1 with the final score of 34.07%**.** Despite there are two Level 4 factors, the final score affected by half of the factors get Level 1 scores. The categories analysis shows as well that two out of three categories scored in Level 1 category with 29.52% and 32%.

It can be seen from the feedback analysis that in this organisation, the case study participants strongly agreed on the assessment of most categories, and despite the final IA score of their organisation was on Level 1 status, they agreed that the final IA score reflected the degree to which the IA implementation was successful in their organisation. Moreover, they concluded that the instrument was a good instrument to measure IA for eGovernment in the Indonesia government organisations.

7.3 The third case study

This organisation is a city government organisation. The government office is in the capital of a province in Indonesia. There were 10 participants involved. One participant was from senior management, three IT management, and six IT staff. The eGovernment was implemented in this organization since 2008 and is one of the best organisations in its performance and adoption of the eGovernment in Indonesia. The results of the study in this organisation are shown below.

7.3.1 The results of the third case study

In this section, the results of the third case study are presented in this section. For Organisational Management (OM) category, the results are shown in Table 7.11.

Table 7.11 The results of the third case study for OM

Cat No	Category Items	Factor No	Factor Items	Instrumental Questions	Scores
1	Organisational Management (OM) Score: 54.29% Response: Strongly Agree	1	Leadership and Commitment	The lead of board of directors to IA implementation?	60%
				The commitment of board of directors to IA implementation?	60%
		2	Policy, Legal, and Compliance	The availability of policy to provide management direction and support for IA in accordance with business requirements?	60%
				The availability of legal aspects to identify the organisation's legal obligation (statutory, regulatory, and contractual)?	60%
				The availability of appropriate procedures to ensure compliance with the legal aspects that apply to the organisation?	60%
		3	Management Review and Continual Improvement	The periodic review (regarding the suitability, adequacy, and effectiveness) of the information assurance policy by senior management?	40%
				The continual improvement of the information assurance policy by senior management?	40%

		4	Holistic Approach	The treatment of IA as a combination of the physical, procedural, personnel, and technical security?	60%
		5	Business Alignment	The alignment between IA implementation and the organisation's business needs?	40%
		6	Organisational Roles, Responsibilities, and Authorities	The senior management assigned and communicated organisational roles relevant to IA?	60%
				The senior management assigned responsibilities for ensuring IA is in accordance with the policy?	60%
				The senior management assigned authorities to confirm information assurance is in accordance with the policy?	60%
		7	Awareness, Education, and Training	The awareness of all employees in the organisation on their contribution to the IA implementation?	60%
				The education of all employees in the organisation as relevant for their job function?	60%
				The training of all employees in the organisation as relevant for their job function?	60%

From the calculation of the 15 Instrumental Questions scores, for the OM category, the final score was 54.29%. This score represents the OM status of their organisation in implementing IA. The participants strongly agreed with this score. Furthermore, Table 7.12 presents the results for the Implementation Management (IM) category.

Table 7.12 The results of the third case study for IM

Cat No	Category Items	Factor No	Factor Items	Instrumental Questions	Scores
2	Implementation Management (IM) Score: 53.33% Response: Agree	1	Risk Management	The adopted of risk management strategy of IA implementation?	60%
		2	Security Objectives	The relevance of information security objectives to the functions and levels.	60%
		3	Operations and Management	The plan of information security complied with information security policy?	60%
				The implementation of information security complied with information security policy?	40%
				The control of information security complied with information security policy?	20%
		4	Performance Evaluation	The performance evaluation (relating to the effectiveness and maintenance) of the IA implementation?	60%
		5	Recovery and Continuity Management	The adopted of disaster recovery plan of IA implementation?	40%
				The adopted of business continuity plan in the event major failures?	40%
		6	Infrastructure Development	The required relevant technology and infrastructure of IA implementation?	60%

The IM category for the third case study, after calculating the scores of nine Instrumental Questions, got a score of 53.33%. The participants strongly agreed to this score. Which means this score

represents IM status in IA implementation in their organisation. Moreover, Table 7.13 presents the results for the Social Management (SM) category.

Table 7.13 The results of the third case study for SM

Cat No	Category Items	Factor No	Factor Items	Instrumental Questions	Scores
3	Social Management (SM) Score: 42% Response: Agree	1	Cultural Issues	The consideration of cultural issues in the organisation during the implementation of IA?	60%
		2	Digital Divide	The consideration of digital literacy issue in the organisation during the implementation of IA?	40%
		3	Trust and Privacy	The established of trust between government and citizens?	40%
				The protection regarding privacy of information?	60%
		4	Organisational Structures	The creation of a division to be in control of handling information security issues?	40%
		5	Coordination	The coordination between institutions regarding the duties of each institution?	20%

The score for the OM category in the second case study is 42%. This score represents the calculation of the scores obtained by answering six Instrumental Questions. The participants strongly agreed that this score represented the OM status for IA implementation in their organisation.

7.3.2 The analysis of the third case study

This section presents factor analysis, categories analysis, and feedback analysis from the third case study.

7.3.2.1 Factors analysis

The results of factor analysis from the third case study are shown in Table 7.14

.

Table 7.14 The factors analysis of the third case study

Factor Category	Factor Name	Factor Status
OM	Leadership and Commitment	Level 3 Factor (60%)
	Policy, Legal, and Compliance	
	Holistic Approach	
	Organisational Roles, Responsibilities, and Authorities	
	Awareness, Education, and Training	
IM	Risk Management	
	Security Objectives	
	Performance Evaluation	
	Infrastructure Development	
SM	Cultural Issues	
SM	Trust and Privacy	Between Level 2 and Level 3 (40%-60%)
OM	Management Review and Continual Improvement	Level 2 (40%)
	Business Alignment	
IM	Operations and Management	
	Recovery and Continuity Management	
SM	Digital Divide	
	Organisational Structures	
SM	Coordination	Level 1 (20%)

7.3.2.2 The categories analysis of the third case study

The radar chart of the categories analysis of the second case study in the Figure 7.3 and a recommendation action suggested based on the results are presented as follows.

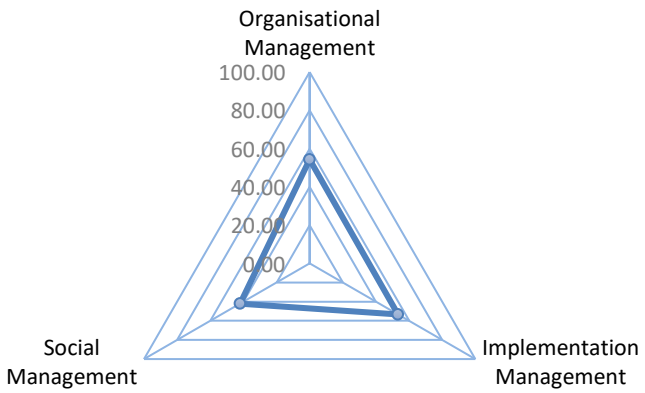

Figure 7.3 The radar chart of the third case study

Level 2 categories:

1. **42%,** Social Management

Level 3 categories:

2. **54.29%,** Organisational Management
3. **53.33%**, Implementation Management

The calculation can be found in Appendix G. Case Studies Calculation

7.3.2.3 Feedback analysis

The feedback analysis and participants' comments on the third case study from the afterthought session from the participants are presented in this section. Table 7.15 below shows the feedback analysis.

Table 7.15 The feedback analysis of the third case study

Questions	Responses
Q1. Organisational Management, 54.29% Q4. Whole IA is Level 2 status, 50.55% Q5. Good Instrument	Strongly Agree
Q2. Implementation Management, 53.33% Q3. Social Management, 42%	Agree

The score of OM category in this organisation is 54.29%. The participants strongly agreed with it. Moreover, they commented that the leadership and commitment of leaders in this organisation are good enough so that the implementation of IA is not disturbed. Then, review of IA has been

conducted regularly and improvement also has been carried out as needed. In addition, the aspects of physical, personnel, technical, and procedures are integrated and support each other. Further, people who are responsible for each position have been appointed by the top management according to their competency.

The score of the IM category is 53.33%. This score is agreed by all participants. They mentioned that risk management has been adopted and implemented properly. And for periodic reviews of performance evaluations, it has been carried out and improvements have also been conducted. Furthermore, this organisation has disaster recovery centres outside the city as part of continuity management to anticipate possible incidents. Additionally, the infrastructure in this organisation is sufficient to support good IA implementation.

The organisation got a score of 42% for the SM category. They agreed to this result as it represented the status of the category in their organisation. In addition, they mentioned that the organisation has policies to address cultural issues such as resistance to change or openness. Moreover, the trust from the public on this organisation is quite good, and also the privacy of the users has been well managed. However, coordination with other institutions, especially the private sector, is not good enough.

Lastly, the whole IA in this organisation is categorised as Level 2 implementation with a score of 50.55%. The score is agreed strongly by the organisation during the afterthought session. They also stated that the instrument is a good instrument for measuring IA for eGovernment in the Indonesian context. Furthermore, they are satisfied with the results and would be interested to take part in the future study.

7.3.3 The discussion of the third case study

In this case, the results revealed that the final score was not affected by the Level 1 factor, as there were many moderate and average factors involved in the study, as well as all-average categories. Hence, the final IA score is Level 2 because of most factors get Level 2 score.

The case study participants in this organisation strongly agreed on the assessment of most categories. This indicates that the organisation agreed on the results and questions. In addition, as they had the highest score of all three case studies, therefore, they are the most advanced and experienced in IA implementation practices in this study. Furthermore, participants agreed that the instrument was an effective instrument for measuring IA for eGovernment in Indonesia.

7.4 Discussion of the findings

This chapter presents a discussion of the findings of the case studies. The case studies were conducted in three government institutions in Indonesia which had been implemented eGovernment services with a varied time period. Group discussions were chosen as the approach to do case studies. Each finding is discussed in detail as follows.

7.4.1 Organisational Management category

The findings indicate that the status of Leadership and Commitment factor for IA implementation in these organisations is moderate. This is based on the average score of all case studies for this factor which is 40 or has an average status. This finding is in line with some reviewed studies which states that although Leadership and Commitment factor is important, the fact is that in Indonesia the commitment of the leadership is still moderate (Furuholt and Wahid, 2008; Koesharijadi, Hardiyansyah and Akbar, 2019). Furthermore, Djumadal (2008) and Anggono (2015) argue that this factor is a challenge for government organisations in Indonesia, especially since leadership affects policies, regulations, supports, as well as commitment. This finding has significant implications for government organisations in Indonesia. Foremost, the result provides a fact that leadership and commitment in government organisations in Indonesia are still moderate. This information can be used by them to make leadership-binding regulations to anticipate things that can happen due to poor leadership and commitment in their organisations, e.g. reducing the budget or stopping support for IA implementation. That way it is expected that their leaders will be willing and able to support the implementation of IA. With good leadership and commitment, success in implementing IA can be achieved.

Further, all case studies also have an average status for Policy, Legal, and Compliance factor. This means that the policy, legal, and compliance aspects in Indonesian government organisations in implementing IA already exist even though they have not been completed and consequently lowering their overall status of IA implementation. This aligns with some studies (Hardjaloka, 2014) which states that there are still many local governments that have not issued a policy or legal for their organisations. Moreover, the finding provides evidence that the awareness of Indonesian government organisations of the importance of policy, legal, and compliance aspects is still inadequate. Therefore, it urges Indonesian government organisations to seriously consider improving policy, legal, and compliance aspects within their IA implementation. By having a policy, they will have a foundation and a clear direction as well as guidance related to the IA implementation (IASME, 2013; ISACA, 2013). Additionally, having a legal aspect is also fundamental to determine the legal, statutory, regulatory or contractual obligations of their organisation.

Moreover, compliance is necessary to prevent them from breach the legal aspect that applies to them.

Next is finding of Management Review and Continual Improvement factor. The finding shows that based on all case studies, this factor has an average score of 30. This means the status of management review and continual improvement for IA policy in Indonesian government organisations is below average. This in line with the study of Setiadi, Sucahyo, Hasibuan (2012), which stated that Indonesian organisations mostly do not review and improve IA policy regularly, especially to anticipate rapid technology development. The organisation from the first case study (see section 7.1.2.3) also stated that there is no policy for periodic review in their organisation. Usually, reviews are carried out in an incidental manner, such as if there is an event or an audit is carried out. And then from the results, improvement will be made. The finding provides an insight that government organisations in Indonesia have a poor management review and continual improvement in their IA implementation. It has significant consequences for them. Firstly, without having periodic reviews, the effectiveness of their IA policy is questionable and will have an impact on the implementation of IA itself. Consequently, they must invest in enabling periodic review and continual improvement. This would be helping them to evaluate the effectiveness, suitability and adequacy of their IA policy and it can help them in achieving successful IA implementation (ISO/IEC 27001, 2013). It should also be noted that all levels of management are made aware of any changes, updates, and revisions.

Moreover, Holistic Approach is another factor that got an average status in all case studies conducted. It means the organisations have treated IA as a unity of the physical, procedural, personnel, and technical security despite not fully complete yet. This is in line with some studies (Anggono, 2014; Chaerudin, 2018) that Indonesian government organisations have tried to integrate human, technical and procedural aspects in implementing IA. This is important for an organisation to be able to manage the risk to the governance, compliance, confidentiality, integrity and availability of its information at all times (Bunker, 2012). This finding has significant ramifications for Indonesian government organisations. In assuring information, organisations are urged to not only focus on the technical aspect and neglect human, physical, and procedural aspects. They should consider integrating all of them. This is because threats do not only come from the technical aspect, in fact, many threats come from the human aspect. By combining all these aspects, it is expected that defences are layered in-depth and the weakness in one aspect can be covered in other aspects.

Furthermore, the average score of Business Alignment factor from all case studies indicates that on average, organisations got a below-average status for this factor. This means IA has not been

projected to support the business needs of the organisations. Organisation from second case study (see section 7.2.2.3) states, they have not included IA aspect when planning business plans. This is in alignment with some studies (Gamaliel, Rindengan, and Karouw, 2017) that say, the maturity level of alignment between IT and business in Indonesian government organisations is low. This finding gives significant insights for Indonesian government organisations. Foremost, they do not understand the value of IA for their business and neglect it. It means IA departments do not have a clear understanding of what is important to the business. Consequently, IA decisions are made separate into business decisions. To solve this, they must start to transition their business plans to include IA as a standalone business function, not just as a separate function in their organisation. Moreover, the organisations also need to ensure that the IA's goals are tied back to overall IT and business-level goals. By doing that, everyone is working towards a common goal. Further, IA supports the business strategy, adds value and drives success. This creates greater integrations and collaboration between departments.

Further, the results of case studies show that Organisational Roles, Responsibilities, and Authorities factors get an average status. This means that government organisations in Indonesia have already defined the roles and assigned the people responsible for implementing IA. However, from the case studies, there are two contradictory conditions. The organisation from the third case study (see section 7.3.2.3) states, that the senior management has assigned people with competency for the roles in implementing IA. On the other side, the organisation from the second case study (see section 7.2.2.3) express, that in their organisation some roles are filled with incompetent people. This is in alignment with some studies that state, one of the biggest weaknesses in government organisations in Indonesia lies in the number and quality of human resources that support each level of management, especially IA (Masyhur, 2013; Operanata, 2015). This finding shows a significant observation in government organisations in Indonesia. This shows that even though they have defined roles and responsibilities for IA implementation, they have not been able to appropriately appoint people who deserve to be in that position. This will have implications for the success or failure of IA implementation in the organisation because without being handled by the right people, IA implementation cannot be achieved (IASME, 2013; ISACA, 2013; ISO/IEC 27001, 2013). To overcome this, senior management must make specific criteria as the basis for the appointment of certain positions, this is so that the people appointed are truly able to carry out their duties and responsibilities. In addition, to overcome the lack of quality and number in human resources, education and training can be other alternatives to utilize existing resources.

Next, the factor of Awareness, Education, and Training is a factor that gets an above-average status. This factor has the highest score in the OM category based on all the case studies that have been

conducted. This finding indicates that socialisation for awareness and provision of education and training in practice has been carried out by organisations to support the competencies of their staff. Even so, the organisation in the first case study (see section 7.1.2.3) says that training is not given regularly but depends on demand. And also, the low level of awareness of IA policy in the second organisation (see Table 7.6), implies that staff are not yet aware of the IA policy and the importance of their contribution to the success of IA implementation. This is in line with some studies that state the lack of competence in human resources becomes a challenge in the implementation of IA (Wicaksono, 2003; Setiadi, Sucahyo & Hasibuan, 2012). Moreover, according to some studies (Ardiyanti, 2014; Operanata, 2015), the lack of awareness in the public sector is another issue as it is important and can be the key element to an effective IA strategy. This finding provides an important understanding of government organisations in Indonesia. In general, the status of awareness, education, and training in government organisations in Indonesia are good. Even so, they should improve their staff awareness by providing socialization and also conducting regular education and training to ensure the competency of their staff.

7.4.2 Implementation Management category

Risk Management is one of the factors that also get above-average status. This indicates that in practice, risk management has been carried out in government organisations in Indonesia. This is in line with several studies (Setiadi, Sucahyo and Hasibuan, 2012; Nurrohmah, Dewi and Sahadi, 2017) which state that government organisations in Indonesia are required to adopt risk management approach and it is generally having a good rating implementation. However, from the third case study (see section 7.3.2.3), the organisation state that even they have been adopted the risk management approach, they have not adopted a certain standard in implementing it. This finding provides significant evidence if the adoption of risk management in government organisations in Indonesia has been good. To improve its status to be better and even complete, it is recommended that they adopt a standard for risk management and also to consider risk management in the business context for providing IA to the business (IASME, 2013).

Furthermore, the average score of Security Objectives factor from all case studies indicates that organisations got an average status for this factor. This means that security objectives in government organisations in Indonesia have been implemented quite well, although not yet comprehensive. The organisation from the first case study mention (see section 7.1.2.3) that for the security objectives aspect, it is already well-designed and also everything is well-monitored. This is in alignment with some studies (Setiawan, 2013; Juliharta, 2019) which state that some government organisations in Indonesia have good information security objectives, despite most

organisations are still at the inadequate level. This finding provides significant evidence for government organisations in Indonesia. This indicates that the conditions of information security in organisations in Indonesia have not been equal. This information can be used by government organisations in Indonesia as a basis for improving their information security. This can be done by evaluating their information security policy and make sure it is relevant to the functions and levels and be consistent with the information security policy. Moreover, with the risk management level that is above average, the security objectives are expected to be more effective, since the needs of information security must consider the results of the risk assessment and risk treatment.

Next is finding of Operations and Management factor. The finding shows that based on all case studies, this factor has an average score of 33.33. This means the status of operations and management for IA policy in Indonesian government organisations is below average. From the second case study (see section 7.2.2.3), the organisation state that the technical implementation of security has been carried out, but the main problem is more on the human aspect. This is in line with some studies that state, the lack of competence related to technical actions and procedures for dealing with security issues is a challenge in Indonesia (Setiadi, Sucahyo & Hasibuan, 2012; Ardiyanti, 2014) and also another challenge from the human aspect is the lack of expertise and awareness level (Operanata, 2015). This finding provides an important insight for government organisations in Indonesia. This implies that even though the plan and procedures for implementation, control, and updates already exist, the capabilities of human resources to execute them is still lacking. As a result, with a lack of capabilities, the implementation of information security will not be optimal. To overcome this, it can be achieved by recruiting new competent staff, or another alternative is by conducting capacity building for existing staff to be able to carry out technical activities in accordance with procedures.

Furthermore, the average score of Performance Evaluation factor from all case studies indicates that on average, organisations got a below-average status for this factor. From the results of the group discussion, for this factor, the organisations from the first and second case studies each got the same score, which is 20 (see

Table 7.1 and Table 7.6). This means performance evaluation on IA has not been conducted properly in these organisations. They state (see section 7.1.2.3 and 7.2.2.3), even they have been doing performance evaluation, it has not been conducting regularly. Consequently, it affects their total score of implementation management category resulting in an average status. This is in line with some studies that state performance evaluation in government organisations in Indonesia is generally available but not yet comprehensive (Nurrohmah, Dewi and Sahadi, 2017). This finding provides significant insight for government organisations in Indonesia. Foremost, it indicates that they need to start doing performance evaluation regarding IA periodically. This factor is important, as the processes include internal audits, monitoring, measurement, analysis, and evaluation, which intended to evaluate the performance and effectiveness of the IA and to ensure if the IA implementation complies with the IA policy (ISO/IEC 27001, 2013).

Moreover, Continuity Management is another factor that got a below-average status in all case studies conducted. It means the organisations have adopted the continuity management factor despite still in the initial stage. Two organisations from case studies (see section 7.2.2.3 and 7.3.2.3) mention that they have disaster recovery centre as part of continuity management, however, it has not been standardised. This is in alignment with finding from other studies that state continuity management in government in Indonesia is already available despite not yet fully complete (Nurrohmah, Dewi and Sahadi, 2017). This finding provides a significant fact that the continuity of management is not yet performing in government organisations in Indonesia. This information has implications if they must begin to consider improving their continuity management adoption. This can be done by starting to standardise their disaster recovery centre and doing periodic backups. It is necessary for organisations to be able to maintain business as usual in the event of major failures or a disaster (IASME, 2013).

Next, the factor of Infrastructures Development is a factor that gets an above-average status. This factor has the highest score in the IM category based on all the case studies that have been conducted. This finding indicates that these organisations generally have adequate infrastructures for implementing IA. However, this result was obtained because these organisations fall into the category of large organisations in Indonesia. One organisation from the case studies state (see section 7.2.2.3) that the infrastructure in their organisation is very good because it is an organisation that has a large budget for infrastructure expenditure. This is in line with some studies (Setiawan, 2013; Nurrohmah, Dewi and Sahadi, 2017) that state, the condition of infrastructure in each government organisation in Indonesia is different, this is due to geographical location and also the budget allocated to build infrastructure in each organisation is different, this is resulting in larger organisations have better infrastructure. Large organisations mainly located in important

cities or provinces and they have a big budget allocation for infrastructure. This finding provides significant evidence for government organisations in Indonesia. This indicates that the conditions infrastructures development in organisations in Indonesia is not equal. To overcome this, smaller organisations and organisations that are located in unimportant cities or provinces, are urged to request assistance from the central government to get additional budgets to build infrastructure. If this is not possible, another alternative is by asking the central government to take over the procurement of infrastructure.

7.4.3 Social Management category

The findings indicate that the status Cultural Issues factor for IA implementation in these organisations is moderate. This is based on the average score of all case studies for this factor which is 40 or has an average status. It means that there are cultural issues in these organisations that have not handled properly. Some of the issues that occur are a reluctance to change or open, as happened in the organisations in the second and third case studies. This finding is in alignment with some studies that state, many government organisations in Indonesia experiencing cultural issues such as no culture of sharing, resistance toward openness, and resistance to change of mindset (Furuholt & Wahid, 2008; Hardjaloka, 2014). This finding provides significant insight for Indonesian government organisations. This information can be used by organisations to design a solution to anticipate cultural issues during IA implementation. They can make policies that force all staff to change their habits so that their actions can positively impact the implementation of IA. Another way is by applying rewards and punishments that will be given as a consequence of their actions based on the report (Furuholt and Wahid, 2008).

Next, the factor of the Digital Divide is a factor that gets a below-average status. This factor has the lowest score in all categories based on all the case studies that have been conducted. From case studies, it was found that digital illiteracy is still common in these organisations due to the incompatibility of the staff background with their positions (see section 7.1.2.3 and 7.2.2.3). This is in line with some studies, that reveal inequality distribution of basic ICT services across districts in Indonesia resulting in uneven competence and affects the achievement of IA (Sujarwoto & Tampubolon, 2016). In addition, around 25% of civil servants in Indonesia categorised as older (BPS-Statistics Indonesia, 2016), and older workers with poor ICT literacy skills are more likely to struggle when new technologies are introduced into workplaces (Eales, Kim & Fast & 2017). This finding provides significant insight for Indonesian government organisations. It gives a fact that digital divide is a common problem in all government organisations in Indonesia. They are urged to close the gaps by providing training and education to improve the digital literacy of their staff. Another

way is by moving old workers who cannot comprehend new technologies to other positions that are easier for them and replacing them with workers who are able to handle new technologies.

Furthermore, the average score of Trust and Privacy factor from all case studies indicate that on average, these organisations got a below-average status for this factor. It means the trust and privacy aspects in these organisations have been handled properly despite not fully complete yet. One organisation state (see section 7.3.2.3) that the privacy of users in their organisation is well-protected, therefore the trust from the public on this organisation is quite good. This is in line with some studies that state, most organisations in Indonesia already have a policy for data privacy. However, the implementation is often relying on organisational policy and regulations from the ministerial level, since data privacy laws and regulations do not exist in Indonesia (Norton Rose Fulbright, 2014). This finding provides a significant fact for Indonesian government organisations. Organisations that do not yet have a policy in protecting data privacy, are urged to start having it and implementing it. With the enormous amount of user information that must be managed, regarding the issue of privacy of information, the government should consider the responsibility with the intention that the user information is well protected (Khalil, Lanvin & Chaudhry, 2002). Moreover, with data privacy is well protected, trust between government institutions as well with the citizens will be successfully achieved in the implementation of eGovernment.

Next is finding of Organisational Structures factor. The finding shows that based on all case studies, this factor has an average score of 40. This means the status of organisational structures for IA policy in Indonesian government organisations is average. This is in line with the study which states that the Indonesian government already has several national scale organisations to deal with information security issues (Setiadi, Sucahyo and Hasibuan, 2012). This finding provides an important fact for Indonesian government organisations. Despite a national-scale organisation is necessary, at the local level there should also be a division with the main duty is maintaining the information security issues for the organisation. Previous finding (see section 5.1.2.1) states that the National security agency is important and needs to be improved like KISA in Korea. Nevertheless, it is impossible if one organisation has to deal with all information security issues. Therefore, information security must be maintained by every government organisation.

Lastly, the average score of Coordination factor from all case studies indicates that on average, these organisations got a below-average status for this factor. It means the coordination within these organisations is poor. The findings from case studies (see section 7.2.2.3 and 7.3.2.3) show that coordination between staff is still poor so there is overlap in work, besides coordination with other organisations is also not good enough. This is in line with previous findings (see section 5.1.2.1) that state, although there are agencies that deal with security issues, in practice agencies like ID-

SIRTI and CERT-ID sometimes do overlapping work, and coordination within organisations needs to be handled properly so that no more additional work or overlap cases. Moreover, previous studies (Operanata, 2015) also state that with many government institutions in Indonesia, there must be coordination between institutions so that the duties of each institution do not overlap in protecting government information as well as eGovernment services. This finding provides significant insight for Indonesian government organisations regarding coordination within their organisations. To deal with this, they can make clear policies, regulations, and procedures regarding the duties of divisions in their organisation, so that no work is being done many times or the worst case is nobody works on it.

7.4.4 Afterthought session

To summary participants' feedback, Table 7.16 presents a comparison of the feedback from the five case studies. In terms of a scoring system for the effectiveness of the instrument, the following system has been established: Strongly Agree (SA) is 5, Agree (A) is 4, Neutral (N) is 3, Disagree (D) is 2 and Strongly Disagree (SD) is 1.

Table 7.16 The summary of case studies feedback

Question	CS 1	CS 2	CS 3	AS
Q1: Organisational Management (OM)	SA	A	SA	4.6
Q2: Implementation Management (IM)	A	SA	A	4.3
Q3: Social Management (SM)	SA	SA	A	4.6
Q4: Whole IA	SA	A	SA	4.6
Q5: Good instrument	SA	SA	SA	5

****CS:*** *Case Study****, AS:*** *Average Score*

The table above shows the answers to questions in the afterthought session. It shows all questions are either strongly agreed or agreed by all participants. The first question, namely "To what extent do you agree with these results reflect the actual status of 'Category X' in your organization?". The average score of the feedback for each category is 4.6, 4.3, and 4.6. Moreover, the second question asked was "To what extent do you agree that these results reflect the actual status of IA in your organisation?" The average score of participants' feedback on the final score is 4.6. These scores mean the results are approved by organisations and it shows the effectiveness of the instrument.

For the last question "To what extent do you agree that this instrument is a good instrument for measuring IA implementation processes for eGovernment in Indonesia?" which is still in the afterthought session, all organisations strongly agreed that the instrument is a good instrument. The average score of the feedback for this category is 5, which means the organisations strongly approved that the instrument is a good instrument measuring IA implementation processes for eGovernment in Indonesia. They also remarked that the instrument is easy to use, and the scale is easy to understand. They also expressed that the study provided them with awareness about the condition of IA in their organisation. In addition, they also provided suggestions for further instrument development. They stated; it would be better if there is a tool to help to decide a score from the metric during the assessment process.

Overall, it may be said that the instrument was able to assess accurately the status of IA implementation in these organisations. Moreover, all participants consider the instrument to be a good instrument to measure IA for eGovernment in government organisations in Indonesia. Thus, it can be concluded that the instrument is effective to measure IA for eGovernment in the Indonesian context.

These results provide significant insight into government organizations in Indonesia. By having accurate results regarding the status of their IA implementation, they can conduct benchmarking to compare their IA implementation process with other organisations. This is intended that an organisation can learn to improve factors that are lacking in their IA implementation from organisations that have succeeded in implementing these aspects. Furthermore, the results of the benchmark can also be used as information for them to make a road map to improve their IA implementation further. In the road map, they can include new policies, procedures, as well as planning for providing training and education based on their needs.

7.5 Study Limitations

In spite of the insights offered by this study into understanding the status of IA implementation for eGovernment in Indonesia, this study has some limitations. First, this instrument was specifically developed to measure the process of implementing IA for eGovernment in Indonesia. Therefore, this instrument might not be possible to measure the IA implementation process in other contexts.

Second, this study focused on the IA implementation for eGovernment only, it suggests that these findings may not be reflective of the status of other IA implementations in a different context.

7.6 Summary

This chapter presented the results and discussed the case studies conducted using the instrument developed based on the IA framework. The case studies were conducted in three government institutions in Indonesia. The institutions had been implemented eGovernment services with a varied time period.

Analysis of case studies showed mixed results. Two organisations got average status for IA implementation in their organisations, while one organisation got the below-average status. Furthermore, all organisations agreed if the results reflected IA implementation status in their organisation.

In addition, they commented on the conditions of IA implementation in their respective organisations. Moreover, they were satisfied with the instrument and stated that the instrument is good and effective for measuring the process of implementing IA for eGovernment in Indonesia. Additionally, they provided suggestions for the further development of the instrument and were interested in participating again in future studies. In summary, it can be concluded that the instrument is effective to measure IA implementation for eGovernment in the Indonesian context.

Chapter 8 Conclusion and Future Work

This chapter provides an overview of this research and the conclusions drawn from it, in addition to the potential future work.

8.1 Conclusion

In summary, eGovernment is an initiative that aims to improve the quality of public services. With the demanded services that must be always available, assuring the continuity of eGovernment services becomes one of the problems in the implementation of eGovernment. One way to guarantee eGovernment service is with the implementation of information assurance (IA). IA performed by combining technological, human, and organisational aspects that have a strong emphasis on strategic risk management. Moreover, IA has a broad connotation that includes reliability, authentication, and nonrepudiation and provides restoration of information systems when an incident occurs, which ensures business continuity. In Indonesia, eGovernment is still in the development stage, and from the literature review, so far there is no IA framework that focuses on assuring eGovernment service in Indonesia. Therefore, the aim of this research is to develop an IA framework for eGovernment within the Indonesian context. It is important to identify factors for effective IA implementation. By identifying factors from international standards as well as IA factors from literature and eGovernment challenges in the Indonesia context, the framework was developed and proposed. The framework consists of 18 factors and categorised into three categories: organisational, implementation, and Indonesian context.

The questions specified in Chapter 1, needing to be answered were:

Q1. What form of IA framework is appropriate for the Indonesian eGovernment?
This question is divided into two sub-questions:

- Q1.1 What are the issues and challenges facing the implementation of IA for eGovernment in Indonesia?
- Q1.2 How can the proposed framework be evaluated to efficiently and appropriately meet the demands in assuring eGovernment services within the Indonesian context?

Q2. How can the IA implementation process for eGovernment within the Indonesian context be measured?

Q3. Is the developed measuring instrument an appropriate instrument to measure the implementation process of IA for eGovernment in government organisations in Indonesia?

The Q1 consists of two sub-questions. The Q1.1 was answered by identifying the factors through reviewing the existing publications on information assurance, presented in Chapter 2.

The Q1.2 was answered in two stages. The first stage was to review the factors that had been identified and explored other factors by interviewing eight experts in the field of IA, eGovernment, and InfoSec from various institutions in Indonesia. The findings revealed that organisational structure factors needed to be improved in scope by adding the need for a division that is responsible for addressing security issues in every institution. In addition, some experts emphasised the need to focus on cultural issues in IA implementation in Indonesia. Furthermore, all experts agreed that all the factors identified are important in IA implementation for eGovernment in Indonesia, despite one expert stated that although the Recovery and Continuity Management factor is important, the Configuration Management Database (CMDB) is more important.

The second phase involved an online survey that was distributed to IA, eGovernment, InfoSec practitioners in Indonesia to confirm the updated framework from the first stage. The results indicated that all factors are statistically significant.

Finally, the Q2 and Q3 were answered by developing an instrument based on the framework and use it to conduct case studies. This stage involved pre-testing and confirming the instrument and then conducting five case studies in government institutions in Indonesia and analysing the case studies. All organisations agreed if the results reflected IA implementation status in their organisation. It means that all the instrument factors and categories reflect the accurate status of IA in these organisations. Moreover, they also remarked that the instrument is easy to use, and the scale is easy to understand. They also expressed that the study provided them with awareness about the condition of IA in their organisation. Hence, the instrument is effective to measure IA for eGovernment in the Indonesian context. In addition, they also provided suggestions for further instrument development. They stated; it would be better if there is a tool to help to decide a score from the metric during assessment process.

Finally, it can be seen that the framework has passed many stages and phases to come to its final shape. Thus, it can be said the framework is validated. Furthermore, the validated framework is shown in Table 8.1.

Table 8.1 The validated IA framework

Cat No	Category	Factor No	Factors
1	Organisational Management	1	Leadership and Commitment
		2	Policy, Legal, and Compliance
		3	Management Review and Continual Improvement
		4	Holistic Approach
		5	Business Alignment
		6	Organisational Roles, Responsibilities, and Authorities
		7	Awareness, Education, and Training
2	Implementation Management	1	Risk Management
		2	Security Objectives
		3	Operations and Management
		4	Performance Evaluation
		5	Recovery and Continuity Management
		6	Infrastructures Development
3	Social Management	1	Cultural Issues
		2	Digital Divide
		3	Trust and Privacy
		4	Organisational Structures
		5	Coordination

Moreover, Table 8.2 shows a summary of the method used to answer Q1, Q2, and Q3 with the purpose of applying them.

Table 8.2 Summary of methods used for answering the research questions

Research Questions	Sub Research Questions	Methods	Purpose	Status
Q1. What form of IA framework is appropriate for the Indonesian eGovernment?	Q1.1 What are the issues and challenges facing the implementation of IA for eGovernment in Indonesia?	Literature review	Identify the factors for information assurance implementation	Completed
	Q1.2 How can the proposed framework be evaluated to efficiently and appropriately meet the demands in assuring eGovernment services within the Indonesian context?	Semi-structured interview with information assurance, eGovernment, and information security experts	1. Assess the importance of each factor found in the literature to the framework 2. Identify additional factors related to the Indonesian context	Completed
		Online survey with IA, eGovernment, and InfoSec practitioners	Confirm the factors identified from literature and experts	
Q2. How can the IA implementation process for eGovernment within the Indonesian context be measured?		Developing an instrument based on the GQM approach	Measure the implementation process of information assurance implementation in Indonesian government organisations	Completed
Q3. Is the developed measuring instrument an appropriate instrument to measure the implementation process of IA for eGovernment in government organisations in Indonesia?		Using the instrument in case studies	Ensure its effectiveness within the Indonesian organisations	Completed

8.2 Contribution summary

8.2.1 Framework

This study presented an IA framework for eGovernment in Indonesia consists of 18 factors by identifying factors which are influenced by IA standard-based frameworks, IA critical success factors, and challenges within the Indonesian context. Thus, these factors are the answer to the Q1.1: "What are the issues and challenges facing the implementation of IA for eGovernment in Indonesia?"

Culturally speaking, IA is rarely addressed by studies in Indonesia in general, and in the eGovernment aspect in particular. Moreover, to the best of my knowledge, there are no studies on the factors of IA for eGovernment in Indonesia. Therefore, this study is one of the first of its kind, referring specifically to IA for eGovernment in Indonesian institutions. The IA framework with 18 factors which has been evaluated and confirmed by experts and practitioners from Indonesia is the answer to the Q1.2: "How can the proposed framework be evaluated to efficiently and appropriately meet the demands in assuring eGovernment services within the Indonesian context?"

8.2.2 Instrument

An instrument was developed in this research based on the confirmed IA framework, in order to measure the success of the implementation of IA in the Indonesian organisations. This instrument has been validated and applied to three case studies of organisations in the public sector in Indonesia. This instrument is the answer to the Q2: "How can the IA implementation process for eGovernment within the Indonesian context be measured?"

Moreover, all participants agreed that all the instrument factors and categories reflect the accurate status of IA in their organisations. Further, all participants consider the instrument to be a good instrument to measure IA for eGovernment in the government organisations in Indonesia. Thus, it can be concluded that the instrument is effective to measure IA implementation for eGovernment in the Indonesian context and answering Q3: "Is the developed measuring instrument an appropriate instrument to measure the implementation success of IA for eGovernment in government organisations in Indonesia?"

Further, this research provides a unique way of showing the assessment results to the participating organisations. The radar charts show the organisations' IA success status in simple terms, by way of a single diagram.

Finally, by successfully answering all the research questions, this study contributed to the IA implementation and eGovernment literature. This work will serve as a basis for researchers to develop more precise IA implementation models for eGovernment. Moreover, the findings of this study will assist policymakers in the IA implementation for Indonesian eGovernment initiatives to set a strong foundation for successful IA implementation.

8.3 Future Work

The previous chapters show that the information assurance framework has been fully confirmed by going through a literature review, reviews from experts as well as a survey with practitioners. Moreover, an instrument also developed and validated through case studies. Therefore, one can conclude that the framework addresses the IA implementation for eGovernment in Indonesia. Further, there are opportunities and improvements can be achieved from this IA framework.

8.3.1 Benchmarking successful IA

The first improvement that can be gained is to use the radar chart, which depicts the results of the assessments, to compare the results of one or more organisations to an organisation with the most successful IA implementation. In Figure 8.1, there are three assessments of three organisations, each represented by a different colour. The benchmarked organisation (Benchmark) is blue, while the others are all different colours. This method gives the organisations an indication of their position with regard to other organisations in the same industry.

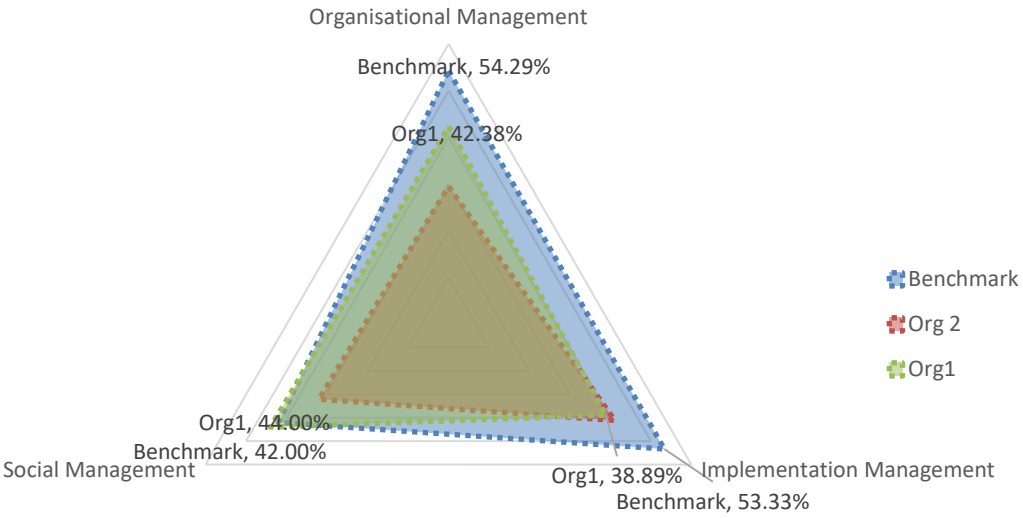

Figure 8.1 IA Benchmarking

8.3.2 Developing a measurement tool

During case studies, participants suggested that it would be better if there is a list of processes or levels to help to decide a score from the metric during assessment process. It can be achieved by developing a measurement tool for capability. Within the scale, the measure of capability is based upon the nine process attributes (PA) defined in ISO/IEC 15504-2. Process attributes are used to determine whether a process has reached a given capability. Each attribute measures a particular aspect of the process capability.

At each level there is no ordering between the process attributes; each attribute addresses a specific aspect of the capability level. The list of process attributes is shown in Table 8.3.

Table 8.3 Capability levels and process attributes

Process Attribute ID	Capability Levels and Process Attributes
	Level 0: Non-existent Process
	Level 1: Initial Process
PA 1.1	Process performance
	Level 2: Defined Process
PA 2.1	Performance management
PA 2.2	Work Products management
	Level 3: Managed Process
PA 3.1	Process definition
PA 3.2	Process deployment
	Level 4: Established Process
PA 4.1	Process measurement
PA 4.2	Process control
	Level 5: Optimized Process
PA 5.1	Process innovation
PA 5.2	Continuous optimization

References

Abu-Musa, A.A., 2007. Exploring Information Technology Governance (ITG) in Developing Countries: AN Empirical Study. Int. J. Digit. Account. Res. 7, 27–51. https://doi.org/10.4192/1577-8517-v7

Alateyah, S., Crowder, R.M. and Wills, G.B., 2012. Towards an integrated model for citizen adoption of E-government services in developing countries: A Saudi Arabia case study. International Journal for Digital Society (IJDS), 3(3/4), pp. 666-676.

Albino, V., Berardi, U. and Dangelico, R. M. (2015) 'Smart cities: definition, deminsion, and performance', journal Urban Technology, 22, pp. 3-21. doi: http://dx.doi.org/10.1080/10630732.2014.942092.

Alfawaz et al., 2007. E-government security in developing countries: A managerial conceptual framework. Information Systems Management, (March), pp. 26-28.

Alshenqeeti, H., 2014. Interviewing as a Data Collection Method: A Critical Review. English Linguistics Research [online], 3 (1), 39-45. Available from: http://www.sciedu.ca/journal/index.php/elr/article/view/4081.

Anderson, C., 2010. Presenting and evaluating qualitative research. American Journal of Pharmaceutical Education, 74 (8).

Anggono, B.D., 2014. Smart city di Indonesia. 7 Novemb.

Anggono, B.D., 2015. eGovernment Indonesia update 2015-2019. Regional training workshop in Asia and the Pacific: Sustainable development and disaster risk management using E-Government. Available at: http://www.unosd.org/index.php?page=view&type=13&nr=36&menu=177

Anthopoulos, L. G. and Reddick, C. G. (2017) 'Smart City and Smart Government: Synonymous or Complementary? Leonidas', in Proceedings of the 25th International Conference Companion on World Wide Web - WWW '16 Companion, pp. 351-355. doi: 10.1145/2872518.2888615.

Ardiyanti, H., 2014. Cyber-security dan tantangan pengembangannya di indonesia (Cyber-security and the development challenges in Indonesia). Politica, 5 (dinamika masalah politik dalam negeri dan hubungan internaisonal), pp. 95-110. Available at: https://jurnal.dpr.go.id/index.php/politica/article/view/336

Ardiyanti, H., 2014. Cyber-security dan tantangan pengembangannya di indonesia. Politica 5, 95–110.

Avgerou, C., 1993. Information systems for development planning. International Journal of Information Management, 13(4), pp. 260-273.

Banerjee, A., Chitnis, U., Jadhav, S., Bhawalkar, J. and Chaudhury, S., 2009. Hypothesis testing, type I and type II errors. Industrial Psychiatry Journal, 18(2), p. 127. Available at: http://www.industrialpsychiatry.org/text.asp?2009/18/2/127/62274

Basili, V. R., Caldiera, G., and Rombach, H. D., 1994. The Goal, Metric, and Question Approach. In Encyclopedia of Software Engineering.

Basu, S., 2004. E?government and developing countries: An overview. International Review of Law, Computers & Technology, 18(1), pp. 109-132. Available at: http://www.tandfonline.com/doi/abs/10.1080/13600860410001674779

Bhattacherjee, A., 2012. Social Science Research: principles, methods, and practices. Textbooks collection.

Birchall, D., Ezingeard, J.-N., McFadzean, E., Howlin, N. and Yoxall, D., 2004. Information assurance: Strategic alignment and competitive advantage. Available at: http://eprints.kingston.ac.uk/5429/

Blyth, A., Kovacich, G.L., 2006. Information Assurance: Security in the Information Environment, 2nd ed, Computer Communications and Networks. Springer, London. https://doi.org/10.1002/9781444312171.ch3

BPS Statistics Indonesia, 2016. Statistical Yearbook of Indonesia 2016. p. 720. Available at: https://www.bps.go.id/website/pdf_publikasi/Statistik-Indonesia-2016--.pdf

Braun, V. and Clarke, V., 2006. Using thematic analysis in psychology. Qualitative Research in Psychology [online], 3 (2), 77-101. Available from: http://eprints.uwe.ac.uk/11735.

Bryman, A. & Cramer, D., 2001. Quantitative Data Analysis with SPSS Release 10 for Windows.

Bullen, C. V. and Rockart, J.F., 1981. A primer on critical success factors. Working papers, (69), pp. 1-64. Available at: http://ideas.repec.org/p/mit/sloanp/1988.html

Bunker, G., 2012. Technology is not enough: Taking a holistic view for information assurance. Information Security Technical Report [online], 17 (1-2), 19-25. Available from: http://dx.doi.org/10.1016/j.istr.2011.12.002.

Burge, R., 2014. Lincolnshire police information assurance strategy, standards and working practices. (June), p. 59. Available at: https://www.lincs.police.uk/media/56634/information-assurance-strategy.pdf

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., and Neville, A. J., 2014. The Use of Triangulation in Qualitative Research. Oncology Nursing Forum [online], 41 (5), 545-547. Available from: http://onf.ons.org/onf/41/5/use-triangulation-qualitative-research.

CCEB, 2015. Information Assurance for Allied Communications and Information Systems.

CESG, 2015. The Information Assurance Maturity Model and Assessment Framework. [online], (2.1). Available from: https://www.ncsc.gov.uk/guidance/information-assurance-maturity-model-and-assessment-framework-gpg-40.

Chaerudin, A., 2018. Strategi Keamanan Siber Nasional.

Cherdantseva, Y. and Hilton, J., 2013. A reference model of information assurance & security. 2013 International Conference on Availability, Reliability and Security, (September), pp. 546-555. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6657288

Cohen, J., 2013. Statistical Power Analysis for the Behavioral Sciences. Hoboken: Taylor and Francis.

Cohen, S. and Eimicke, W., 2002. The future of E-Government: A project of potential trends and issues. In: Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS-36). p. 146b (1-10). Available at: http://csdl2.computer.org/persagen/DLAbsToc.jsp?resourcePath=/dl/proceedings/hicss/&toc=comp/proceedings/hicss/2003/1874/05/1874toc.xml&DOI=10.1109/HICSS.2003.1174327

COBIT 5, 2013. COBIT 5 for Assurance.

Cope, C., 2015. 10 Principles for effective information assurance.

CSIA. (2007). A National Information Assurance Strategy.

Curtin, G.G., 2007. E-Government. Encyclopedia of political communications, (April), pp. 200-204. Available at: http://bedrosian.usc.edu/files/2012/07/encyclopedia_of_political_communications.pdf

Dahlan, N., 2008. Development of e-Government in Indonesia: A Strategy Model and Its Achievements. Ritsumeikan J. Asia Pacific Stud. 24.

Denzin, N.K., 1978. Sociological methods: A sourcebook. New York, NY: McGraw-Hill.

Djumadal, J. S. (2008). Implementasi E-Government, Sebuah Harapan Penuh Tantangan Di Provinsi Daerah Istimewa Yogyakarta. In Konferensi dan Temu Nasional Teknologi Informasi dan Komunikasi untuk Indonesia.

DTI, 2006. Information security: Protecting your business assets. Available at: http://webarchive.nationalarchives.gov.uk/20060213212102/dti.gov.uk/bestpractice/assets/security/ispyba.pdf

Eales, J., Kim, C., Fast, J., 2017. How deep is the digital divide? ICT literacy and the role of assistive technology in helping older workers. FACTS.

Ebrahim, Z., Irani, Z., 2005. E-government adoption: Architecture and barriers. Bus. Process Manag. J. 11, 589–611. https://doi.org/10.1108/14637150510619902

Edwards, R. and Holland, J., 2013. What is Qualitative Interviewing? [online]. 'What is?' Research Methods Series. Available from: https://books.google.com/books?redir_esc=y&id=GdCOAQAAQBAJ&pgis=1.

Erzberger, C. and Prein, G., 1997. Triangulation: Validity and empirically-based hypothesis construction. International Journal of Methodology [online]. Available from: http://link.springer.com/article/10.1023/A:1004249313062.

European Smart Cities (2015) European Smart Cities 4.0. Available at: http://www.smart-cities.eu/?cid=01&ver=4 (Accessed: 16 April 2019).

Ezingeard, J.-N., McFadzean, E. and Birchall, D., 2005. A model of information assurance benefits. Information Systems Management, 22(2), pp. 20-29.

Fang, Z., 2002. E-Government in digital era: Concept, practice, and development. 10(2), pp. 1-22.

Faul et al., 2009. Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. Behavior Research Methods, 41(4), pp. 1149-1160. Available at: http://www.springerlink.com/index/10.3758/BRM.41.4.1149

Faul, F., Erdfelder, E., Buchner, A., and Lang, A.-G., 2009. Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. Behavior Research Methods [online], 41 (4), 1149-1160. Available from: http://www.springerlink.com/index/10.3758/BRM.41.4.1149.

Field et. al. 2013. Discovering Statistics Using SPSS. Sage (Vol. 81). https://doi.org/10.1111/insr.12011_21

Furuholt, B., Wahid, F., 2008. E-Government Challenges and the Role of Political Leadership in Indonesia: the Case of Sragen. Proc. 41st Annu. Hawaii Int. Conf. Syst. Sci. (HICSS 2008) 1–10. https://doi.org/10.1109/HICSS.2008.134

Gamaliel, B., Rindengan, Y., Karouw, S., 2017. Pengukuran Tingkat Keselarasan Tata Kelola Teknologi Informasi Menggunakan COBIT 5 Pada Pemerintah Sulawesi Utara. E-Journal Tek. Inform. 11.

Gil-Garcia, J. R., Helbig, N. and Ojo, A. (2014) 'Being smart: Emerging technologies and innovation in the public sector', Government Information Quarterly. Elsevier Inc., 31(S1), pp. I1-I8. doi: 10.1016/j.giq.2014.09.001.

Gil-Garcia, J. R., Zhang, J. and Puron-Cid, G. (2016) 'Conceptualizing smartness in government: An integrative and multi-dimensional view', Government Information Quarterly. Elsevier Inc., 33(3), pp. 524-534. doi: 10.1016/j.giq.2016.03.002.

Guenduez, A. A. et al. (2018) 'Smart Government Success Factors', Swiss Yearbook of Administrative Sciences, 9(1), pp. 96-110. doi: 10.5334/ssas.124.

Guenduez, A. A., Mettler, T. and Schedler, K. (2017) 'Smart Government - Partizipation und Empowerment der Bürger im Zeitalter von Big Data und personalisierter Algorithmen', HMD Praxis der Wirtschaftsinformatik, 54(4), pp. 477-487. doi: 10.1365/s40702-017-0307-4.

Guest, G., 2006. How many interviews are enough? An experiment with data saturation and variability. Field Methods, 18(1), pp. 59-82. Available at: http://fmx.sagepub.com/cgi/doi/10.1177/1525822X05279903

Hall, E.T., 1976. Beyond culture. Contemporary Sociology.

Hardjaloka, L., 2014. Studi Penerapan E-Government di Indonesia dan Negara Lainnya Sebagai Solusi Pemberantasan Korupsi di Sektor Publik. RechtsVinding, 3(3).

Hibbard, E.A., 2009. Introduction to Information Assurance. Storage Networking Industry Association. Available at: http://www.snia.org/sites/default/education/tutorials/2009/spring/security/EricHibbard-Introduction-Information-Assurance.pdf

Hofstede, G., 2001. Culture's Consequences: Comparing Values, Behaviors, Institutions and Organizations Across Nations, 2nd ed. Thousand Oaks, CA: SAGE Publications.

Hukum Online., 2014. Keamanan Informasi e-Gov Masih Rentan. [online] Available at: https://www.hukumonline.com/berita/baca/lt540fe9fedd278/keamanan-informasi-ieGov-i-masih-rentan [Accessed 27 Aug. 2018].

IASME, 2013. The Standard for Information Assurance for Small and Medium Enterprises (IASME). (2.3).

Indrajit, R.E., 2006. Electronic Government Konsep Pelayanan Publik Berbasis Internet dan Teknologi Informasi. Aptikom.

Irawanto, D.W., 2016. An Analysis of National Culture and Leadership Practices in Indonesia. J. Divers. Manag. 4, 41. https://doi.org/10.19030/jdm.v4i2.4957

ISO/IEC 27001:2013, 2015. ISO/IEC 27001:2013. (September 2014).

Jaeger, P.T. and Thompson, K.M., 2003. E-government around the world: Lessons, challenges, and future directions. Government Information Quarterly, 20(4), pp. 389-394.

Johnson, R. B. and Onwuegbuzie, A. J., 2004. Mixed Methods Research: A Research Paradigm Whose Time Has Come. Educational Researcher [online], 33 (7), 14-26. Available from: http://www.jstor.org/stable/3700093.

Joseph, R.C., 2009. Government-to-business (G2B) perspectives in E-Government. Northeast Decision Sciences Institute Proceedings, pp. 192-199.

Juliharta, I.G.P.K., 2019. Analisa tingkap kesiapan penerapan keamanan teknologi informasi dalam pelaksanaan e-government berbasis indeks keamanan informasi (kami) studi kasus pemerintah kota kediri. J. Teknol. Inf. dan Komput. 5, 21–27.

Jupp, V., 2006. The Sage dictionary of social research methods. Sage.

Karokola et al., 2011. Secure e-Government services: Towards a framework for integrating IT security services into e-Government maturity models. In: Information Security South Africa (ISSA) 2011.

Karokola, G.R., 2012. A framework for securing e-Government services: The case of Tanzania. Available at: http://www.diva-portal.org/smash/get/diva2:557279/FULLTEXT04.pdf

Khalil, M.A., Lanvin, B.D. and Chaudhry, V., 2002. The E-Government handbook for developing countries. A project of InfoDev and the Center for Democracy & Technology, (November).

Kociemba, M., 2015. Fundamental security concepts. John Hopkins, Available at: http://dx.doi.org/10.1007/978-1-4615-1663-7_16

Koesharijadi, Hardiyansyah, Akbar, M., 2019. Implementasi kebijakan e-government, komitmen, pengembangan aparatur dan implikasinya terhadap kinerja pelayanan publik 3, 39–45.

Kominfo, 2010. Indonesia ICT Whitepaper. Pusat Data Kementrian Komunikasi dan Informatika.

Kominfo, 2012. Pemeringkatan e-Government Indonesia (Indonesian e-Government Ranking). Direktorat e-Government. Kementrian Komunikasi dan Informatika.

Kominfo, 2015. ICT Research and Development in Indonesia. Bangkok.

Kothari, C. R., 2004. Research Methodology: Methods & Techniques. New Age International (P) Ltd.

Lambrinoudakis et al., 2003. Security requirements for e-government services: A methodological approach for developing a common PKI-based security policy. Computer Communications, 26(16 SPEC.), pp. 1873-1883.

Lazar, J., & Preece, J., 2002. Social considerations in online communities: Usability, sociability, and success factors.

Leung et al., 2005. Culture and international business: Recent advances and their implications for future research. Journal of International Business Studies, 36(4), pp. 357-378. Available at: http://link.springer.com/10.1057/palgrave.jibs.8400150

Likert, R., 1932. A technique for the measurement of attitudes. Archives of Psychology, 140, 1-55.

Liu, P., Yu, M. and Jing, J., 2006. Information assurance. Handbook of information security: Information warfare, social, legal, and international issues and security foundations, Vol. 2.

Lombardi, P. et al. (2012) 'Modelling the smart city performance', Innovation, 25(2), pp. 137-149. doi: 10.1080/13511610.2012.660325.

Masyhur, F., 2013. The Role of Human Resources in The Implementation of E-Government in Parepare / Peran Sumber Daya Manusia Dalam Implementasi E-Government PERAN SUMBER DAYA MANUSIA DALAM IMPLEMENTASI E-GOVERNMENT PADA PEMERINTAH KOTA PAREPARE THE ROLE OF HUMAN RESOURCES I.

May, C. (CERT/CC T. and E.C.), 2006. Defense in Depth: Foundation for Secure and Resilient IT Enterprises. (September), p. 346. Available at: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA460375

MICT, 2014. National information assurance policy 2.0. CNSS Instruction No. 4009, CNSSI No. (4009).

Miles, M. and Huberman, A., 1994. Qualitative Data Analysis. Thousand Oaks: Sage.

Muller, L., 2015. Cyber security capacity building in developing countries: Challenges and opportunities. Norwegian Institute of International Affairs, (21), pp. 1-4. Available at: http://nynorsk.nupi.no/index.php/content/download/497977/1662177/version/1/file/NUPI+Report+03-15-Muller.pdf

Napierala, M., 2012. What Is the Bonferroni Correction?? AAOS Now [online], April, 1-3. Available from: http://www.aaos.org/news/aaosnow/apr12/research7.asp.

Ndou, V., 2004. E-Government for developing countries: Opportunities and challenges. The Electronic Journal on Information Systems in Developing Countries, 18(1), pp. 1-24. Available at: http://www.ejisdc.org

Norton Rose Fulbright, 2014. Global Data Privacy. Global Data Privacy Directory [online], 1-206. Available from: http://www.nortonrosefulbright.com/files/global-data-privacy-directory-52687.pdf.

Nurrohmah, I., Dewi, M.A.A., Sahadi, N., 2017. Measuring the e-Government Maturity in Indonesia using the Ranking of e-Government of Indonesia (PeGI). Am. Sci. Res. J. Eng. Technol. Sci. 32, 49–63.

OECD, 2003. The case for E-Government: Excerpts from the OECD report: The E-Government imperative. OECD Journal on Budgeting, 3(1), pp. 1987-1996.

Operananta, L., 2015. Cyber security: Indonesia's challenges and opportunities to move forward.

Palupy, H. E., 2011. Privacy and Data Protection?: Indonesia Legal Framework. Universiteit van Tilburg.

Palvia, S.C.J. and Sharma, S.S., 2007. E-Government and E-Governance: Definitions/domain framework and status around the world. Foundations of E-government, pp. 1-12.

Presiden Republik Indonesia, 2003. Kebijakan dan Strategi Nasional Pengembangan E-Government. Instruksi Presiden Republik Indonesia Nomor 3 Tahun 2003. Available at: http://simkum.baliprov.go.id/uploads/INPRES_3_2003.doc%5Cnhttp://dishut.jabarprov.go.id/data/menu/INPRES2003_003.pdf

Priyambodo, T.K. and Prayudi, Y., 2015. Information security strategy on mobile device based eGovernment. ARPN Journal of Engineering & Application Science, 10(2), pp. 652-660.

Puspitasari, L. and Ishii, K., 2016. Digital divides and mobile Internet in Indonesia: Impact of smartphones. Telematics and Informatics [online], 33 (2), 472-483. Available from: http://dx.doi.org/10.1016/j.tele.2015.11.001.

Qu, S. Q. and Dumay, J., 2011. The qualitative research interview. Qualitative Research in Accounting & Management [online], 8 (3), 238-264. Available from: http://www.emeraldinsight.com/doi/10.1108/11766091111162070.

Rathmell, A., Daman, S., O'Brien, K. and Anhal, A., 2004. Engaging the board corporate governance and information assurance. Information Assurance Advisory Council (IAAC).

Recker, J., 2012. Scientific research in information systems: a beginner's guide. Springer Science & Business Media.

Rogers, Y., Sharp, H., and Preece, J., 2011. Interaction Design: Beyond Human-Computer Interaction. Wiley.

Romney et al., 1986. Culture as consensus: A theory of culture and informant accuracy. American Anthropologist, 88(2), pp. 313-338.

Rugman, A. M. and Collinson, S., 2006. International Culture. International business, 129-158.

Saunders, M., Lewis, P. and Thornhill, A., 2009. Research Methods for Business Students. Pearson, New York.

Schedler, K. (2003) 'Local and regional public management reforms in Switzerland', Public Administration, 81(2), pp. 325-344. doi: 10.1111/1467-9299.00349.

Scholl, H. J. and Scholl, M. C. (2014) 'Smart Governance: A Roadmap for Research and Practice', (1). doi: 10.9776/14060.

Schostak, J., 2006. Interviewing and representation in qualitative research [online]. 1st ed. British Educational Research Journal. Maidenhead: Open University Press. Available from: http://www.sciedu.ca/journal/index.php/elr/article/view/4081.

Schware, R. (Ed.), 2005. E-development from excitement to effectiveness. Available at: http://documents.worldbank.org/curated/en/2005/01/6399566/e-development-excitement-effectiveness

Seifert, J.W., 2003. A primer on e-Government: Sectors, stages, opportunities, and challenges of online governance. Report for Congress, p. 24.

Setiadi, F., Sucahyo, Y. G., and Hasibuan, Z. A., 2012. An Overview of the Development Indonesia National Cyber Security. International Journal of Information Technology & Computer Science (IJITCS), 6, 106-114.

Setiadi, F., Sucahyo, Y.G. and Hasibuan, Z.A., 2013. Balanced E-Government security framework: An integrated approach to protect information and application. In: Proceedings of 2013

International Conference on Technology, Informatics, Management, Engineering and Environment, TIME-E 2013.

Setiawan, A.B., 2013. Kajian Kesiapan Keamanan Informasi Instansi Pemerintah Dalam Penerapan E-Government. J. Masy. Telemat. dan Inf. 4, 109–126.

Silcock, R., 2001. What is E-government? Parliamentary Affairs, 54, pp. 88-101. Available at: http://pa.oxfordjournals.org/content/54/1/88.abstract%5Cnhttp://pa.oxfordjournals.org/content/54/1/88.full.pdf%5Cnhttp://pa.oxfordjournals.org/content/54/1/88.short%5Cnhttp://pa.oupjournals.org/cgi/doi/10.1093/pa/54.1.88

Smircich, L., 1983. Concepts of Culture and Organizational Analysis. Concepts Cult. Organ. Anal. 28, 339–358. https://doi.org/10.4324/9781315241371-20

Sipatuhar, I.S. and Sutaryo, 2016. Faktor-Faktor Penentu Implementasi E-Government Pemerintah Daerah di Indonesia. Simposium Nasional Akuntansi XIX, pp. 24-27.

Sujarwoto, S. and Tampubolon, G., 2016. Spatial inequality and the Internet divide in Indonesia 2010-2012. Telecommunications Policy [online], 40 (7), 602-616. Available from: http://dx.doi.org/10.1016/j.telpol.2015.08.008.

Sujarwoto, S., Tampubolon, G., 2016. Spatial inequality and the Internet divide in Indonesia 2010–2012. Telecomm. Policy 40, 602–616. https://doi.org/10.1016/j.telpol.2015.08.008

Tannahill, C., 2013. Information Assurance Strategy NHS Lanarkshire. (4).

Tashakkori, A., & Teddlie, C., 2010. SAGE handbook of mixed methods in social and behavioral research (2nd ed.). Thousand Oaks, CA: Sage.

Tavakol, M. and Dennick, R., 2011. Making sense of Cronbach's alpha. International journal of medical education, 2, 53-55.

Turnbull, N., 2003. 'Foreword' In A. Calder and S. Watkins, IT Governance: A manager's guide to data security S BS 7799/ISO 17799 (2nd ed.), Kogan Page (Set Book).

United Nations., 2018. E-Government Survey 2018: Gearing E-Government to support transformation towards sustainable and resilient societies. New York 270. https://doi.org/e-ISBN: 978-92-1-055353-7

Upadhyaya, P., Shakya, S. and Pokharel, M., 2012. Security Framework for E-Government Implementation in Nepal. Journal of Emerging Trends in Computing and Information Sciences, 3(7), pp. 1074-1078. Available at: http://www.cisjournal.org

U.S. Department of Defense (DOD). (2007). Directive Number 8500.01E October 24, 2002 (Certified Current as of April 23, 2007). 980(8570), 1–10. Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/471511p.pdf

Venkatesh, V. and Brown, S. A., 2013. Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems. MIS Quarterly Vol. X No. X, pp. 1-XX/Forthcoming 2012-2013, X (X), 1-34.

Walsham, G., Symons, V. and Waema, T., 1988. Information systems as social systems: Implications for developing countries. Information Technology for Development, 3(3), pp. 189-204. Available at: http://www.tandfonline.com/doi/abs/10.1080/02681102.1988.9627126

Wang, H., & Rubin, B. L. (2004). Embedding e-finance in e-government: a new e-government framework. Electronic Government, an International Journal, 1(4), 362-373.

Wicaksono, D. A. (2003). E-Government in Indonesia : the Opportunities and Challenges. Development, 1-2.

Willke, H. (2007). Smart governance. Frankfurt: Campus Verlag.

Wirtz, B.W. and Daiser, P., 2015. E-Government - Strategy process instruments. Available at: http://www.uni-speyer.de/files/de/Lehrstühle/Wirtz/WirtzDaiser_2015_E-Government.pdf

World Bank, 2008. Technology & Development. Global Economic Prospects 2008: Technology Diffusion in the Developing World.

World Bank. (2015). e-Government. [online] Available at: http://www.worldbank.org/en/topic/ict/brief/e-government [Accessed 9 Feb. 2017].

Yalman, Y. and Yesilyurt, M., 2013. Information security threats and information assurance. TEM Journal, 2(3), pp. 247-252.

Yanqing, G., 2010. E-government: Definition, goals, benefits and risks. 2010 International Conference on Management and Service Science, MASS 2010, pp. 9-12.

Yanti, M. and Alamsyah, A., 2014. Determinant of digital divide in Indonesia: the case of South Sumatera Province. Afro Asian Journal of Social Sciences [online], 5 (1), 1-28. Available from: http://www.onlineresearchjournals.com/aajoss/art/130.pdf.

Yeasmin, S. and Rahman.K.F, 2012. ' Triangulation ' Research Method as the Tool of Social Science Research. Bup Journal [online], 1 (1), 154-163. Available from: http://www.bup.edu.bd/journal/154-163.pdf.

Yin, R., 2003. Case Study Research: Design and Methods. Sage, Los Angeles.

Zareen et al., 2013. Cyber security challenges and way forward for developing countries. pp. 7-14.

Appendix

A. Participation Information Sheet 1

Participant Information Sheet

Study Title: Factors affecting the implementation of information assurance for eGovernment in Indonesia
Researcher: Rio Guntur Utomo
ERGO number: ERGO/FPSE/29459
Please read this information carefully before deciding to take part in this research. It is up to you to decide whether or not to take part. If you are happy to participate you will be asked to sign a consent form.
What is the research about?
This research is for my PhD project, which is to construct an information assurance framework for eGovernment in Indonesia. The aim of this study is to investigate the factors affecting the implementation of information assurance for eGovernment in Indonesia.
Why have I been asked to participate?
You have been approached because of your experience in information security, information assurance or eGovernment.
What will happen to me if I take part?
If you decide to take part in this research you will spend about 20 minutes for completing the questionnaire or answering the questions in an interview format.
Are there any benefits in my taking part?
Participants will not be directly benefited by taking part in this research project.
Are there any risks involved?
No risks are involved in this research.
Will my participation be confidential?
All date collected will be anonymous. Collected information will be stored and used on secure systems and will be used for this study purpose only and are voluntary and will be confidential. The collection of data complies with the University of Southampton policy under the Data Protection Act.

What should I do if I want to take part?
Participants should inform the researcher if they want to take part in this research after being approached.
What happens if I change my mind?

You have the right to terminate your participation in the research, at any stage, you do not need to give any reasons, and without your legal rights being affected. Your data will be deleted directly if you decide to withdraw at any time.

What will happen to the results of the research?

The research will be published in conferences or journals. Participant will be given a copy of the results if requested. The data will be stored during the study and will be destroyed after the study finished.

Where can I get more information?

Should you need more information, contact me if possible (Rio Guntur Utomo, rgu1n15@soton.ac.uk), otherwise please contact my supervisors, Dr Robert Walters (rjw1@ecs.soton.ac.uk) or Dr Gary Wills (gbw@ecs.soton.ac.uk).

What happens if something goes wrong?

Should you any concern or complaint, contact me if possible (Rio Guntur Utomo, rgu1n15@soton.ac.uk), otherwise please contact my supervisors, Dr Robert Walters (rjw1@ecs.soton.ac.uk) or Dr Gary Wills (gbw@ecs.soton.ac.uk). You can also contact the FPSE Office (ergopse@soton.ac.uk) or any other authoritative body such as the Research Integrity & Governance Team (rgoinfo@soton.ac.uk)

Thank you for taking the time to read the information sheet and considering taking part in the research.

B. Participation Information Sheet 2

Participant Information Sheet

Study Title: Measuring the implementation process of information assurance for eGovernment in Indonesia

Researcher: Rio Guntur Utomo

ERGO number: ERGO/FPSE/41817

Please read this information carefully before deciding to take part in this research. It is up to you to decide whether or not to take part. If you are happy to participate you will be asked to sign a consent form.

What is the research about?

This research is for my PhD project, which is to construct an information assurance framework for eGovernment in Indonesia. The aim of this study is to investigate the factors affecting the implementation of information assurance for eGovernment in Indonesia.

Why have I been asked to participate?

You have been approached because of your role in the institution which implement information assurance for eGovernment.

What will happen to me if I take part?

If you decide to take part in this research, you will spend about 130 minutes for participating in a focus group discussion and answering the questionnaire aftermath.

Are there any benefits in my taking part?

Participants will not be directly benefited by taking part in this research project.

Are there any risks involved?

No risks are involved in this research.

Will my participation be confidential?

All date collected will be anonymous. Collected information will be stored and used on secure systems and will be used for this study purpose only and are voluntary and will be confidential. The collection of data complies with the University of Southampton policy under the Data Protection Act.

What should I do if I want to take part?

Participants should inform the researcher if they want to take part in this research after being approached.

What happens if I change my mind?

You have the right to terminate your participation in the research, at any stage, you do not need to give any reasons, and without your legal rights being affected. Your data will be deleted directly if you decide to withdraw at any time.

What will happen to the results of the research?

The research will be published in conferences or journals. Participant will be given a copy of the results if requested. The data will be stored during the study and will be destroyed after the study finished.

Where can I get more information?

Should you need more information, contact me if possible (Rio Guntur Utomo, rgu1n15@soton.ac.uk), otherwise please contact my supervisors, Dr Gary Wills (gbw@ecs.soton.ac.uk) or Dr Robert Walters (rjw1@ecs.soton.ac.uk).

What happens if something goes wrong?

Should you any concern or complaint, contact me if possible (Rio Guntur Utomo, rgu1n15@soton.ac.uk), otherwise please contact my supervisors, Dr Gary Wills (gbw@ecs.soton.ac.uk) or Dr Robert Walters (rjw1@ecs.soton.ac.uk). You can also contact the FPSE Office (ergopse@soton.ac.uk) or any other authoritative body such as the Research Integrity & Governance Team (rgoinfo@soton.ac.uk)

Thank you for taking the time to read the information sheet and considering taking part in the research.

C. Consent Form

CONSENT FORM

Study title: Factors affecting the implementation of information assurance for eGovernment in Indonesia

Researcher name: Rio Guntur Utomo

Supervisors: Dr Robert Walters and Dr Gary Wills

ERGO number: ERGO/FPSE/29459

Please initial the box(es) if you agree with the statement(s):

I have read and understood the information sheet (2017/07/12, Version 1) and have had the opportunity to ask questions about the study.	
I agree to take part in this research project and agree for my data to be used for the purpose of this study.	
I understand my participation is voluntary and I may withdraw at any time for any reason without my rights being affected.	

Data Protection

I understand that information collected about me during my participation in this study will be stored on a password protected computer and that this information will only be used for the purpose of this study. All files containing any personal data will be made anonymous.

Name of participant (print name)……

Signature of participant……

Date……

D. Interview Analysis

Code	Themes	Expert
Leadership and Commitment	Leadership and commitment determine the organisation's maps and plans.	1
	Of these 18 factors, leadership plays a major role. Because if the leadership is weak, then the implementation will not run successfully. Then the commitment is also important, in the absence of a commitment, then planned projects, including information assurance, will not work.	2
	Important, because if the leadership does not support and does not commit, then the implementation will not run properly.	3
	Leadership and commitment affect the success or failure of information assurance implementation. Because if there is no commitment, then the implementation of information assurance will not be supported properly and might be stopped in the middle of the process.	4
	The leader must commit and support the implementation.	5
	Leadership and commitment influence the implementation of information assurance. If they are not committed e.g., do not provide the resources, then the implementation process will not succeed.	6
	Leadership and commitment affect the information assurance implementation, the absence of these factor might make the implementation will not happen.	7
	Leadership and commitment are the factors that make policy and then down to plan and finance. Do not just agree but not commit. This means there must be a full support, do not just give orders but do not give support.	8
Policy, Legal, and Compliance	Very important. Because these three elements affect the implementation of IA.	1
	Policy, legal, and compliance are related. Commitment turns into policy. To force the organisation to implement and make the system run. And legal is important, because if there is no legal, it will not run.	2

	Yes, implementation should be legalised. Because to be implemented with no problem, policy and legal are necessary and must refer to the both aspects.	3
	In Indonesia, usually policy and legal are already exists, but to comply with the standards has not been carry out.	4
	This factor is important. But usually when the leader changes, there will be politics and interests that can change the policy.	5
	Very important. Because the organisation must provide policy and legal aspects.	6
	Policies and legal are essential for implementation in order to run and must be compliant as well.	7
	Important. Because if you look at the policy, in the government there is a long term, short term and work plan set. And need legal clarity to be implemented.	8
Management Review and Continual Improvement	Management review and continual improvement are important, but we cannot measure things which are still on going, as it usually can be measured when it is done. But we can create an instrument to measure when the process when it is still running, it is called key performance indicator.	1
	This factor is important and usually the board level will appoint senior management to review and report to the board.	2
	In my organisation there is PME (Plan, Monitoring, Evaluation) usually every three months. Technically, monitoring and evaluation are conducted, and reports are made. Then, if there is any shortcoming, it will be evaluated and improved.	3
	This is important. Because sometimes organisational changes will also have an impact on implementation changes.	4
	This is important. In Jakarta every five years there is a review. However, in my opinion it is still lacking. Should be once a year. Because if just every five years, it will accumulate too many things that must be evaluated.	5
	Very important. Management review is required to improve information assurance.	6
	Important. The policy of information assurance should be reviewed periodically and should be improved from the review results.	7

	Important. Because if you look from the program there should be an evaluation process. And there is also an annual report to be evaluated so that next year there is an improvement.	8
Holistic Approach	Important. Can be like PPT (People, Performance, Technology).	1
	Certainly. All aspects must be integrated and become a unity in the implementation process.	2
	Important. In this organisation, there are physical protection, procedure and personnel.	3
	Very important. Because all of these aspects must be integrated into one and cannot be separated.	4
	This is important, because everything must be integrated so that the goal is achieved.	5
	Yes, these aspects must be fulfilled and become a unity.	6
	I have experienced it; all of these elements must be synergised for implementation to run well.	7
	Important. Must be integrated. For example, if procedures exist but not physically supported, it will not work. And if the personnel exist but the procedure does not exist, nor will it work. So, all those components are mutually supportive for the information assurance process.	8
Business Alignment	Important. In addition, to achieve it, organisations must pay attention to business needs, understand subject matters, suitable assessment, criteria and assess.	1
	Important. Information assurance should be able to accommodate business needs.	2
	Important, and leadership affects this because it determines the organisation's policy regarding the business direction.	3
	Information assurance must be aligned with business needs.	4
	Important. Information assurance should be able to support the business processes of the organisation.	5
	Yes, information assurance must be able to support business needs.	6
	Certainly. Because information assurance should be able to accommodate business needs as a supporter.	7
	Important. Business here is the context of the program. Yes, must be aligned as supporting. Supporting or strategy to achieve its business.	8

Organisational Roles, Responsibilities, and Authorities	Important. To determine the direction of the organisation is the responsibility of board levels. Top management (senior management) function is to run PBRM (Plan Build Run Monitoring). While the board runs EDM (Evaluate Directing Monitoring). So, for this factor, the management is the one who responsible.	1
	Important. It is necessary. Because the role of each responsible division must be clear. Then, if a system is assigned to a division, it must be clear who is responsible for it. Moreover, there must be a legal aspect as well as a commitment.	2
	In the organisation here, the tasks are given to the work units with their respective responsibilities.	3
	State civil apparatus in Indonesia is required to legally have functional position within the organisation.	4
	Important and to be top management, they must have qualifications and certifications.	5
	Very important, because organisations must have people who perform the main tasks and functions in accordance with their role in the organisation.	6
	Board members should appoint people and provide roles with authority and responsibility to them.	7
	Because each personnel have their respective roles. The task corresponds to the direction or policy set by top management.	8
Awareness, Education, & Training	Very important. Because if the staff has no knowledge, then they must be educated and if they are not competent, then they should be trained.	1
	Important. And they are also must aware of what is being implemented (objective). Because although there is a policy, it can be a bottle neck at the staff level for the reason that they are not used to it.	2
	Each staff must be competent in their respective fields and aware of the policies and duties.	3
	For the current policy, there are already laws that state that the civil apparatus of the state has to be competence in their field. In addition, every staff should be aware of the policy as well.	4

	Ideally all layers must be aware of the policy. And all should have standardisation for their competence.	5
	All staff should be aware and competent in their field by receiving education and training. And all staff must be aware of policy.	6
	Although the staff is not yet fully competent, it's fine. But must be aware first. Competence can be obtained from training and education as well as socialization.	7
	All must be competent. One way for the judgment or justification is with a certification. And all staff also must be aware.	8
Risk Management	Risk cannot be eliminated but can be minimised. Risk can be transferred, accepted, mitigated, or avoided.	1
	The risk is not just related to system changes. Also, the risk of culture. Because the system may change but the work culture does not change. So, the organisation should be able to manage it.	2
	It is necessary, organisations must be able to manage risk.	3
	Organisations must have risk management.	4
	Organisations must be able to manage risk. Starting from assessment, plan, until treatment. This is important so that the implementation in the future are ready to face the risks.	5
	Risk must be managed properly.	6
	Risk must be taken into account and be managed.	7
	There should be treatment according to the risks. If within the project management, risks will be analysed, after that, a risk management strategy will be developed. Then talk about programs, there must be risks, and risks can be technical or policy.	8
Security Objectives	Objectives must be determined, and to overcome changes in the middle of the process then there should be control and update.	1
	The objectives of security must be determined and aligned with the needs at the beginning.	2
	Security plans and objectives are important in organisations to address security issues.	3
	Important. Especially for the critical as the data from the user.	4
	Objectives must be in accordance with the plan at the beginning. And when there are changes must be able to adapt the changes.	5
	The objective of the security must be relevant to its level.	6

	The objective of security must be relevant to its function and consistent with the policy.	7
	The program is made referring to the master plan, strategic plan, and finally down to the program. So, it must be in accordance with the objective on the master plan.	8
Operations and Management	Control and update must exist as part of the implementation and to ensure it is aligned with the plan.	1
	It should be ascertained in accordance with what is written in the master plan. Because of this the plan has been written on the policy side. So, the implementation must be in accordance with what has been planned and controlled properly.	2
	This factor is important; usually this is a part of PME (Planning, Monitoring, and Evaluation).	3
	Important, from plan to implementation must be in accordance with the policy or standard.	4
	Control from start of plan to implementation is required. As well as if there is an update.	5
	There should be control and updates to fulfil the requirement.	6
	Every implementation should start from planning and there should be control and update.	7
	Plan down to the implementation program, then there is evaluation in the form of control, then there must be an update process. There should be a Plan, Do, Check process.	8
Performance Evaluation	Important. First the need to make the characteristics first, then there is self-assessment, after that the internal audit.	1
	Important, it is very important there should be monitoring and evaluation.	2
	Those who do this are the PME division. There are two aspects being monitored and evaluated here, namely performance and administrative. And there is also internal audit from the inspectorate.	3
	The performance of the information assurance should be evaluated in order to remain effective and in accordance with the policy.	4
	Important. And ideally should follow the international standard. But some organisations are still blind to these standards.	5

	The performance of information assurance must be evaluated to ensure its effectiveness is maintained.	6
	Certainly. There should be an evaluation of how the implementation of the information assurance.	7
	Yes, very important. Because to check the success of the implementation there must be a process of monitoring, evaluation, and must have its measurement, and analysis.	8
Recovery and Continuity Management	CMDB. Configuration Management Database. It is more important. The people are there. The map is there. If a process breaks down it can be known what can be disturbed.	1
	Yes important, the government of Bandung have a disaster recovery centre and placed in a far place.	2
	Very important and already done. The data here are backed up outside the city.	3
	Important. Because if there is an incident that makes a service disturbed then there must be a countermeasure plan to keep the service running.	4
	Important. Because it must be backed up so that recovery and continuity management is guaranteed.	5
	Very important. In Indonesia there are a government regulation that says every organisation must have a business continuity plan.	6
	Certainly. A backup plan should be prepared to keep the business running.	7
	Very important. In addition to securing the data, it should be able to save the data as well.	8
Cultural Issues	Important. Even so, usually in big cities, they have begun to deal with cultural problems.	1
	Each government agency has a different culture and it is unique. For example, when a new system is implemented, resistance to change often occurs.	2
	We ever wanted to implement a new technology but the people in the organisation were hard to accept the new technology. So, there is a need of socialization.	3
	At the time of implementation, local products are often not easy to be implemented. But if the product is a foreign product, it will be	4

	easily accepted. Because of pride. And resistance to change is also happening. The solution can be from top management that forces with policy.	
	Communication between institutions already exists, but the problem is in humans. Like there are, who does not want to share and also some people prefer to use conventional way. Many also are still have old-fashioned habits.	5
	The habits of Indonesians can affect the organization's performance and information assurance. From the bureaucracy, it is so complicated in data sharing. So, there must be rules that force to change the culture.	6
	Most influential aspects are like trust and behaviour issues.	7
	Important. Because cultures cannot change that fast. Like, a change of leadership can change the policy. There are operation standards, but they are not doing it. So, the consideration of existing habits in Indonesia is influential. For example, everything is complete, like the rules. But they do not do it because of their habits.	8
Infrastructures Development	Important. Certainly, it requires good infrastructures.	1
	Important. If the infrastructure is not provided, then the eGovernment will not be able to run and the information assurance cannot be implemented.	2
	Infrastructure must be good. Otherwise, it will interfere with the implementation.	3
	Yes, very important. Because without infrastructure it cannot be in implementation.	4
	Infrastructures development in Indonesia has not been evenly distributed. And should have their own infrastructure. It is not recommended to use a third party. Because for the government, the safe and secure must be guaranteed as well as its privacy.	5
	Very important. Excellent infrastructure is required.	6
	Important. Infrastructure must meet the needs. And infrastructure in Indonesia is not evenly distributed.	7
	If infrastructure is not good, then it cannot support implementation. And there must be infrastructure development.	8

Digital Divide	Important. Because in Indonesia, the technology acceptance is not the same in every city. For example, Jakarta and Papua has different level of technology.	1
	If for example the central government wants to implement into each region, this is very influential because each region has different technological achievements.	2
	Gap acceptance of technology in Indonesia is very large. Access of technology is not evenly distributed and become our problem as well. Therefore, the government has the NP (National Priorities) program. Our activity should refer to the NP, and NP referring to the GAP (Government Activities Plan). The government supports research activities for the outer regions. Namely appropriate technology for equity of technology.	3
	I have experience in Sumatra. To apply the information system alone was difficult, let alone information assurance. Because it deals with the affordability of infrastructure. Therefore, some areas still accept less technology.	4
	The treatment of people from different regions is also different. Different culture differences treatment and approach.	5
	Inadequate technological achievements affect the acceptance of technology in each region.	6
	For race and ethnicity, they are not too critical. But indeed, the technology gap becomes an influential in the acceptance of information and implementation of information assurance. This can be due to the geographical factor as well.	7
	With technological gaps or uneven information gains will lead to uneven competence. Each region has a different vision of technology, so it will have an effect.	8
Trust & Privacy	The government must protect the privacy of the citizen data so that the trust of the citizen will arise.	1
	Yes. And it's protected by Law. So, there are restrictions on information that can be accessed to protect privacy. Like data from National ID cards, not all fields are accessible, only a few common fields can be accessed to protect the privacy of citizens.	2

	Yes, it is important. Trust must exist from the public and the government must protect user data.	3
	The government must guarantee critical data are protected and do not misused by unauthorised parties.	4
	Security must be guaranteed, so that the public trust the government. And there must be a collaborative action between citizens and government.	5
	There is a regulation of Minister of Communications and Informatics which reads every provider of electronic data must be able to protect user data.	6
	Citizens trust must be paid with the government able to protect their data.	7
	Very important. Moreover, the issue is about privacy. Example, electronic national ID card, those are strategic data. The server does not exist in Indonesia. Then, the infrastructure does not match the specifications specified so its security is not guaranteed. If data are being stored in other parties, it can be used by unauthorised or abused parties. It could be mined and exploited by others.	8
Organisational Structures	Important and needs to be improved like KISA in Korea. However, if one organisation has to deal with all information security issues, I do not agree. Because, information security must be maintained by each organisation.	1
	This is important, but it needs to clarify the main tasks and functions.	2
	It is necessary. Because there is a need of a command for information security problem handling.	3
	Important. To ensure information security in every government institution in Indonesia.	4
	There is a need of an organisation to handle security/assurance issues	5
	It is important to handle security/information assurance issues for eGovernment. In Indonesia, they just created a State Code and Cyber Agency to filter information from outside and handle security problems. In Indonesia there are several organizations that monitor the internet, but they work independently. So, when there are incidents and reports, they do not know what to do. Therefore, the	6

	creation of State Code and Cyber Agency is intended to become an organisation that oversees and coordinates them.	
	Although there should be a national-scale organisation deal with security issues, at the local level it should also exist.	7
	Important. Like the American NSA, there is a special government organisation for dealing with security issues.	8
Coordination	Important. In order that each institution tasks do not overlap	1
	Important. So, there will be no overlap.	2
	Yes, this should be there. So, there is coordination in handling security issues.	3
	Important. Nevertheless, in practice, ID-SIRTII and CERT are sometimes overlapping, and the government has made an effort to arrange both to clarify its responsibilities and scope.	4
	There must be coordination between organisations that handle security / assurance.	5
	There must be a coordination. Therefore, inter-institution jobs do not overlap.	6
	Any institution that handles the relevant field, there must be a coordination to avoid overlap in the work.	7
	Important. In order to not add additional works due to overlap. Example, they do the work that has already done.	8

E. Survey Design

Study title: Factors affecting the implementation of information assurance for eGovernment in Indonesia

Researcher name: Rio Guntur Utomo

Supervisors: Dr Robert Walters and Dr Gary Wills

ERGO number: ERGO/FPSE/29459

Questionnaire II (For Information Security, Information Assurance or eGovernment practitioners in Indonesia)

The main aim of this research is to construct the framework of information assurance for eGovernment in Indonesia. You have been chosen because you are a practitioner in information security, information assurance or eGovernment. This research is seeking your opinion about factors affecting information assurance implementation for eGovernment in Indonesia. The questionnaire is divided in to two parts. The first part is designed for collecting general information. The second part is designed for finding out your opinion about factors affecting information assurance implementation for eGovernment in Indonesia.

This research is under the direction of Electronic and Computer Science, University of Southampton. I would appreciate your response to the following questions. Your information will be used for the research purpose only. Thank you very much for your time in completing this questionnaire.

Section A: General Information

Explanation: This section is used to collect your general information. Please consider all the options in each question carefully.

4. **What industry sector do you work in?**

   _____

5. **Do you have any experience in the fields of Information Security, Information Assurance or eGovernment?**

   □ Information Security

   □ Information Assurance

   □ eGovernment

   □ All of them

   □ Other _____

6. **How many years of experience do you have in the field you mentioned above?**

   □ Less than two years

   □ Two years

□ **Two years to five years**

□ **More than five years**

Section B: factors affect information assurance implementation for eGovernment in Indonesia.

To what extent do you agree that the following factors affect information assurance implementation for eGovernment in Indonesia	Strongly Disagree	Disagree	Agree	Strongly Agree
Organisation Management				
1. Leadership in the organisation is critical in the implementation of information assurance.				
2. Commitment from the board level is critical for the achievement of information assurance through the initial planning.				
3. Information assurance policy is important in providing management direction and a guide for meeting organisational objectives.				
4. Legal aspects are important in identifying the organisation's legal obligation (statutory, regulatory, and contractual).				
5. Compliance is necessary to ensure the organisation follows the legal aspects that apply to the organisation.				
6. Senior management should periodically review (regarding the suitability, adequacy, and effectiveness) of the information assurance policy.				
7. Senior management should continually improve the information assurance policy.				
8. The information assurance shall be treated as a combination of the physical, procedural, personnel, and technical security.				
9. The information assurance should be able to accommodate business needs.				
10. Senior management must ensure roles in the organisation to confirm information assurance is in accordance with the policy.				
11. Senior management must assign the responsibility for ensuring information assurance is in accordance with the policy.				
12. Senior management must assign the authority to confirming information assurance is in accordance with the policy.				
13. People who work in the organisation must be aware of the information assurance policy.				
14. People who work in the organisation must be aware of its contribution to the effectiveness and performance of the information assurance.				
15. All employees should be competent in their respective fields.				

16. All employees of the organisation shall receive appropriate education as relevant for their job function.				
17. All employees of the organisation shall receive appropriate training as relevant for their job function.				
18. All employees of the organisation shall receive appropriate regular updates in the organisational policy as relevant for their job function.				
Implementation Management				
19. The organisation should understand the risk to the business information.				
20. The organisation should undertake risk assessment to the business information.				
21. The organisation should manage the risk to the business information.				
22. Information security objectives must be determined relevant to the functions and levels.				
23. Information security objectives must be consistent with the information security policy.				
24. The organisation must ensure the plan of information security to comply with information security policy.				
25. The organisation must ensure the implementation of information security to comply with information security policy.				
26. The organisation must ensure the control of information security to comply with information security policy.				
27. The organisation must ensure the update needed to comply with information security policy.				
28. Internal audits need to be carried out to confirm whether the information assurance complies with the needs of the organisation and the international standards.				
29. Performance evaluation need to be undertaken to ensure the effectiveness and maintenance of information assurance.				
30. Monitoring need to be undertaken to evaluate the effectiveness and maintenance of information assurance.				
31. Measurement need to be undertaken to evaluate the effectiveness and maintenance of information assurance.				
32. Analysis need to be undertaken to evaluate the effectiveness and maintenance of information assurance.				
33. The integrity and availability of information systems must be maintained during an incident or disaster.				

34. Business continuity must be maintained and work as usual in the event of major failures of information systems.				
Indonesian Context				
35. Cultural issues in organisations in Indonesia can affect information assurance performance.				
36. Cultural issues in organisations in Indonesia need to be considered in the implementation of information assurance.				
37. Implementation of eGovernment requires good infrastructures to able to provide services as intended.				
38. Information security process requires good infrastructures to be achieved in accordance with the security objectives.				
39. Differences in geography in Indonesia, have resulted in the emergence of the gap in access to technology.				
40. The gap in access to technology should be addressed regarding information assurance performance.				
41. Trust must be established between government institutions.				
42. Trust must be established between government and citizens.				
43. The government should ensure that the user information is well protected.				
44. The creation of an organisation like a National Cyber Agency to be in control of handling information security issues is required.				
45. The creation of a division such as an information security division to be in control of handling information security issues within an organisation is required.				
46. There must be coordination between institutions so that the duties of each institution do not overlap in protecting eGovernment information.				

After Thoughts	**Yes**	**No**	**Maybe**
47. Do you think the framework represents good fundamental guidelines for the implementation of information assurance for eGovernment in Indonesia?			
48. Do you think the framework is useful in the implementation of information assurance for eGovernment in Indonesia?			
49. Is there anything you would like to add?			

F. Instrument Design

Study title: Measuring the implementation process of information assurance for eGovernment in Indonesia

Researcher name: Rio Guntur Utomo

Supervisors: Dr Gary Wills and Dr Robert Walters

ERGO number: ERGO/FPSE/41817

Questionnaire

The main aim of this research is to construct the framework of information assurance for eGovernment in Indonesia. You have been chosen because you are an employee in a government institution that implement information assurance for eGovernment. This research trying to obtain the status of IA implementation process in your organisation and to obtain your opinion on the IA status of your organisation and the IA for eGovernment measuring instrument. The questionnaire is divided in to two parts. The first part is designed to attain the status of IA implementation process in your organisation. The second part is designed for finding out your opinion about the IA status of your organisation and the IA for eGovernment measuring instrument.

This research is under the direction of Electronic and Computer Science, University of Southampton. I would appreciate your response to the following questions. Your information will be used for the research purpose only. Thank you very much for your time in completing this questionnaire.

Section A: Information Assurance Process Status

Explanation: This section is used to collect your organisation information assurance process status. Please consider all the options in each question carefully, and tick only one answer.

Cat No	Category Items	Factor No	Factor Items	Instrumental Questions	Non-existent	Initial	Defined	Managed	Established	Optimised
1	Organisational Management (OM)	1	Leadership and Commitment	The lead of board of directors to IA implementation.						
				The commitment of board of directors to IA implementation.						
		2	Policy, Legal, and Compliance	The availability of policy to provide management direction and support for IA in accordance with organisation's business requirements.						
				The availability of legal aspects to identify the organisation's legal obligation (statutory, regulatory, and contractual).						
				The availability of appropriate procedures to ensure compliance with the policy and legal aspects that apply to the organisation.						
		3	Management Review and Continual Improvement	The periodic review (regarding the suitability, adequacy, and effectiveness) of the information assurance policy by senior management.						

				The continual improvement of the information assurance policy by senior management.						
		4	Holistic Approach	The treatment of IA as a combination of the physical, procedural, personnel, and technical security.						
		5	Business Alignment	The alignment between IA implementation and the organisation's business needs.						
		6	Organisational Roles, Responsibilities, and Authorities	The senior management assigned and communicated organisational roles relevant to IA.						
				The senior management assigned responsibilities for ensuring IA is in accordance with the policy.						
				The senior management assigned authorities to confirm information assurance is in accordance with the policy.						
		7	Awareness, Education, and Training	The awareness of all employees in the organisation on their contribution to the IA implementation.						
				The education of all employees in the organisation as relevant for their job function.						

				The training of all employees in the organisation as relevant for their job function.						
2	Implementation Management (IM)	1	Risk Management	The adopted of risk management strategy in IA implementation.						
		2	Security Objectives	The relevance of information security objectives to the functions and levels.						
		3	Operations and Management	The plan of information security complied with information security policy.						
				The implementation of information security complied with information security policy.						
				The control of information security complied with information security policy.						
		4	Performance Evaluation	The performance evaluation (relating to the effectiveness and maintenance) of the IA implementation.						
		5	Recovery and Continuity Management	The adopted of disaster recovery plan of the IA implementation.						
				The adopted of business continuity plan of the IA implementation.						

		6	Infrastructure Development	The required relevant technology and infrastructure of IA implementation.						
3	Social Management (SM)	1	Cultural Issues	The consideration of cultural issues in the organisation during the implementation of IA.						
		2	Digital Divide	The consideration of digital literacy issue in the organisation during the implementation of IA.						
		3	Trust and Privacy	The established of trust between government and citizens.						
				The protection regarding privacy of information.						
		4	Organisational Structures	The established of a division to be in control of handling information security issues.						
		5	Coordination	The coordination between institutions regarding the duties of each institution.						

Section B: After Thoughts

Explanation: This section is used to obtain your opinion on the organisation information assurance process status. Please consider all the options in each question carefully, and tick only one answer.

Questions	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
To what extent do you agree that these results reflect the actual status of Organisational Management in your organisation?					
To what extent do you agree that these results reflect the actual status of Implementation Management in your organisation?					
To what extent do you agree that these results reflect the actual status of Social Management in your organisation?					
To what extent do you agree that these results reflect the actual status of IA in your organisation?					
To what extent do you agree that this instrument is a good instrument for measuring IA implementation process for eGovernment in Indonesia?					

G. Case Studies Calculation

1. Calculation of the first case study

The score of each category were calculated as explained below:

1. Organisational Management (OM) weight = (Factor 1 score + … + factor 7 score) / No of the factors in SA (7)
   OM weight = (40 + 40 + 30 + 60 + 40 + 46.67 + 40) / 7 = **42.38%**
2. Implementation Management (IM) weight: (Factor 1 score + … + factor 6 score) / No of the factors (6)
   IM weight: (40 + 40 + 33.33 + 20 + 40 + 60) / 6 = **38.89%**
3. Social Management (SM) weight: (Factor 1 score + … + factor 5 score) / No of the factors (5)
   SM weight: (40 + 20 + 60 + 60 + 40) / 5 = **44%**

Furthermore, the final score of IA in this case study were calculated based on the results of each category. The steps are illustrated below.

1. The factor weight = 100/ (No. of the factors in all categories: 7+6+5) = 100/18 = **5.56**
2. Organisation Management (OM) weight = 5.56 * 7 = **38.9%**
   Implementation Management (IM) weight = 5.56 * 6 = **33.3%**
   Social Management (SM) weight = 5.56 * 5 = **27.8%**
3. OM weight = (Category Weight (38.9) * OM final score in this case study (42.38))/100 = **16.49%**
   IM weight = (Category Weight (33.3) * IM final score in this case study (38.89))/100 = **12.95%**
   SM weight = (Category Weight (27.8) * SM final score in this case study (44))/100 = **12.23%**
4. The total weights of all categories in this case study = 16.49% + 12.95% + 12.23% = **41.67%**

Based on the assessments of the categories and the factors, the final score of whole IA in this case study is **41.67%**, "**Level 2 status, medium improvement is needed**".

2. Calculation of the second case study

The score of each category were calculated as explained below:

1. Organisational Management (OM) weight = (Factor 1 score + … + factor 7 score) / No of the factors in SA (7)
   OM weight = (20 + 33.33 + 20 + 20 + 20 + 33.33 + 60) / 7 = **29.52%**

2. Implementation Management (IM) weight: (Factor 1 score + … + factor 6 score) / No of the factors (6)

   IM weight: (60 + 40 + 26.67 + 20 + 20 + 80) / 6 = **41.11%**

3. Social Management (SM) weight: (Factor 1 score + … + factor 5 score) / No of the factors (5)

   SM weight: (20 + 20 + 60 + 20 + 40) / 5 = **32%**

Furthermore, the final score of IA in this case study were calculated based on the results of each category. The steps are illustrated below.

1. The factor weight = 100/ (No. of the factors in all categories: 7+6+5) = 100/18 = **5.56**
2. Organisation Management (OM) weight = 5.56 * 7 = **38.9%**
   Implementation Management (IM) weight = 5.56 * 6 = **33.3%**
   Social Management (SM) weight = 5.56 * 5 = **27.8%**
3. OM weight = (Category Weight (38.9) * OM final score in this case study (29.52))/100 = **11.48%**
   IM weight = (Category Weight (33.3) * IM final score in this case study (41.11))/100 = **13.69%**
   SM weight = (Category Weight (27.8) * SM final score in this case study (32))/100 = **8.90%**
4. The total weights of all categories in this case study = 16.49% + 12.95% + 12.23% = **34.07%**

Based on the assessments of the categories and the factors, the final score of whole IA in this case study is **34.07%**, "**Level 1 Status, major and urgent improvement is needed**".

3. Calculation of the third case study

The score of each category were calculated as explained below:

1. Organisational Management (OM) weight = (Factor 1 score + … + factor 7 score) / No of the factors in SA (7)

   OM weight = (60 + 60 + 40 + 60 + 40 + 60 + 60) / 7 = **54.29%**

2. Implementation Management (IM) weight: (Factor 1 score + … + factor 6 score) / No of the factors (6)

   IM weight: (60 + 60 + 40 + 60 + 40 + 60) / 6 = **53.33%**

3. Social Management (SM) weight: (Factor 1 score + … + factor 5 score) / No of the factors (5)

   SM weight: (60 + 40 + 50 + 40 + 20) / 5 = **42%**

Furthermore, the final score of IA in this case study were calculated based on the results of each category. The steps are illustrated below.

1. The factor weight = 100/ (No. of the factors in all categories: 7+6+5) = 100/18 = **5.56**

2. Organisation Management (OM) weight = 5.56 * 7 = **38.9%**
   Implementation Management (IM) weight = 5.56 * 6 = **33.3%**
   Social Management (SM) weight = 5.56 * 5 = **27.8%**
3. OM weight = (Category Weight (38.9) * OM final score in this case study (54.29))/100 = **21.12%**
   IM weight = (Category Weight (33.3) * IM final score in this case study (53.33))/100 = **17.76%**
   SM weight = (Category Weight (27.8) * SM final score in this case study (42))/100 = **11.68%**
4. The total weights of all categories in this case study = 16.49% + 12.95% + 12.23% = **50.55%**

Based on the assessments of the categories and the factors, the final score of whole IA in this case study is **50.55%**, "**Level 2 status, medium improvement is needed**".