International Journal on Advanced Science Engineering Information Technology

Vol.10 (2020) No. 3
ISSN: 2088-5334

A Framework for Factors Influencing the Implementation of Information Assurance for e-Government in Indonesia

Rio Guntur Utomo[a,1], Gary Wills[a,2], Robert Walters[a,3]

[a] *School of Electronics and Computer Science, University of Southampton, Southampton, SO17 1BJ, United Kingdom*
E-mail: [1]rgu1n15@soton.ac.uk; [2]gbw@soton.ac.uk; [3]rjw5@soton.ac.uk

***Abstract*— Electronic government (e-Government) enables outstanding improvements to be made to services for the public by the government. This is achieved through improvements to service quality and availability for which access can be given regardless of place and time. In Indonesia, the implementation of e-Government is still not extensively comprehensive and yet being optimized. To support e-Government 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. However, so far, there has not been any research that has focused on IA for Indonesian e-Government. Therefore, this paper researches the factors which influence the implementation of IA in Indonesia to support e-Government. A framework is proposed and consists of three categories: Indonesian Context, Implementation Management, and Organizational Management. The framework was developed through the identification of the factors from IA international standards, international publications, and various challenges. Furthermore, the framework was reviewed and confirmed by surveying practitioners, and interviewing experts in the IA, information security, and e-Government fields in various Indonesian institutions. The results were analyzed by conducting the non-parametric test. In addition, Cronbach's alpha test was used for testing the data reliability. The results demonstrate that every proposed factor in the framework is significant.**

***Keywords*— information assurance; information security; e-government, Indonesian e-government.**

I. INTRODUCTION

The term e-Government is used for defining the total interactions between government agencies, organizations, and the public via information technology (IT) [1]. E-Government implementation has many benefits, such as improved service quality where e-Government systems permit the government, businesses, and the public to get constant access to government information [2]. Additionally, government agency performance in providing customers with public services will bring greater effectiveness and efficiency [3]. Implementing e-Government will increase service, efficiency, and transparency to the public, reduce transaction costs, and add economic benefits [4].

The concept of e-Government in Indonesia refers to using information and communications technology (ICT) in government organizations' servicing procedures [5]. In Indonesia, implementing Government initiatives began in 2003 with the publishing of the Presidential Decree No. 3 [6]. Despite Government benefits, issues also exist regarding it being implemented. Service availability raises concerns [7]. Additionally, Basu [8] states that assurance of communication security and its sources is also an issue. The main concerns of users are in regard to the communicated information integrity. Moreover, e-Government relies on information services and systems, where it has greater vulnerability to threats and requires protection [9].

Consequently, Indonesian e-Government services must be protected and guaranteed. This can be solved by implementing information assurance (IA) to protect information systems and services. IA protects businesses by lowering the risks posed by information [10]. This is performed through cost-effectiveness as well as risk analysis with systematic and comprehensive security countermeasure management [11]. IA is reliant upon many related organizational controls and actions as a model of defense in depth [12]. Every IA process is provided with the aim of supporting corporate governance [13]. With business continuity and services assured, it is predicted that the implementation of e-Government services in Indonesia will be successfully assured; thus, e-Government will improve the quality of service, efficiency, and effectiveness for citizens.

Furthermore, in addition to the technical security aspects, there is variation in the culture of nations, which contributes to real and significant differences in how people work and

how companies operate [14]. It is, therefore, crucial to gain some understanding of the practices and cultures which exist in the implementation of IA in government agencies. Thus, it is necessary for a study to be conducted on the implementation of IA for e-Government in Indonesia. After a review of previous research, as far as we know, no research discusses IA for e-Government in an Indonesian context. Thus, this research aims to investigate the organizational, implementation, and social factors linked to IA adoption in Indonesia to support the e-Government implementation. Hence, this research is also expected to fill the gaps in current study pertinent to the influential factors on the implementation of IA for e-Government in Indonesia government organizations, since Indonesia as a developing country located in the Southeast Asia region has a unique approach that arises from its cultural context.

The paper structure is as follows: The first section presents the state-of-the-art for the adoption of IA in Indonesia government organizations. The second section consists of the literature review of IA principles by different industry standards, and the critical review of the relevant research in IA, information security, and e-Government implementation cases in other countries in general and in Indonesia in particular. Further, the third section presents the developed IA framework. Next, the methodology used in this study is presented in section four. Lastly, section five and six present our findings with a discussion of the results and conclusion of the study.

II. Material and Method

E-Government's main aim is serving its citizens and aiding communications between government organizations and citizens. The best e-Government definition might be: "The use of IT to improve the quality of government information and services to the public to be more efficient, cost-effective, and convenient and to make government more accountable, responsive, and transparent" by The World [15]. Additionally, e-Government needs to concentrate on five government-to-consumer relationships: Government-to-non-profit, Government-to-employees, Government-to-citizens, Government-to-business, and Government-to-government [16].

The Committee on National Security Systems (CNSS) provided a best practice definition of information assurance (IA) as follows: "Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities" [17].

IA has a wider scope compared to information security. Generally, information security places a greater focus on prevention and protection, whilst IA focuses on integrating reaction, detection, and protection [18]. Moreover, information security focuses more on availability, integrity, and confidentiality, whilst IA, which emphasizes a stronger focus on strategic risk management, has wider connotations, including nonrepudiation, authentication, and reliability [10]. IA's purpose is ensuring the non-repudiation, availability, confidentiality, authentication, and integrity of information systems [18].

A. Review of Related Works

Research into the information assurance (IA) framework for Indonesian e-Government does not yet exist, and up to now, there has been little research into IA for e-Government. However, since information security remains a part of IA, and that security cannot be separated from E-Government implementation; therefore, this section discusses the current models and frameworks of both IA and information security. Some research has identified IA or information security issues in the implementation of e-Government.

Based on the Public Critical Infrastructure (PCI), Lambrinoudakis et al. [19] proposed a security policy model. This focused on e-Government information systems and security mechanisms related to the e-Government hardware/software infrastructure. Yet, this study does not identify the model's management and human aspects. Alfawaz, May, and Mohanak [20] identified the e-Government security differences between developing and developed countries and indicated that there are differences. Even though the technology is mostly identical, environmental differences might affect the failure or success of the e-Government implementation. Using a case study in Nepal, Upadhyaya, Shakya & Pokharel [21] developed an e-Government security framework. This framework is for developing countries and is a cost-effective security framework. The framework identified the following factors: infrastructure, training, awareness, and management.

To secure e-Government processes and systems, Setiadi, Sucahyo & Hasibuan [22] used a security framework. The framework is comprised of both non-technical and technical aspects for e-Government security solutions. Priyambodo and Prayudi [23] suggested an information security strategy for mobile-based e-Government systems. The security strategy covers human, service, policy, and technology infrastructure aspects. Yet, the research does not mention risk management and incident handling to maintain e-Government business continuity.

Wang and Sun [24] suggested a framework for an e-Government information security assurance system. Three aspects were used in the research to analyze e-Government information security risks: laws, technology, and management. Karokola, Kowalski, and Yngström [25] suggested a framework to integrate the e-Government maturity model and IT security services. This addressed non-technical and technical factors required for e-Government services. Nonetheless, this does not identify infrastructure and cultural factors.

B. Factors for Successful Information Assurance Implementation

The ISO and IEC developed and published the ISMS standard ISO/IEC 27001: 2013. The standard has guidelines to integrate ISMS with organizational strategies using ten basic requirements [9]. These requirements are Improvement, Performance Evaluation, Operation, Support, Planning, Leadership, Context of the Organization, Terms and definitions, Normative references, and Scope.

The IASME document guides SMEs on assessing and acknowledging business information security maturity levels. IASME applies a control set to every business type and adjusts its implementation irrespective of the risk profile of

the business. For implementation to be effective, IASME has its basis in 12 factors [26]. The 12 factors are as follows: Continuity, Organization, Risk, Policy and compliance, Planning, Assets, People, Access, Physical and environmental, Operations, Disruption, and Incident management.

Additionally, COBIT 5 is a framework of models analytical tools, practices, and principles, which is accepted worldwide. The COBIT 5 is constructed on the COBIT 5 framework's seven-common management and governance enablers [27], as follows: Organizational structures, policies, ethics, Culture, behavior, Processes, Principles, and frameworks, Services, Information, infrastructure, and applications, people, competencies and skills.

Even though these factors stem from international standards, other factors need to be identified from the relevant literature which complements aspects of IA, which the standards do not cover. Bullen and Rockart [28] state that critical success factors (CSFs) have limitations and need to be correctly implemented for organizations to reach their aims and objectives. An ideal CSF implementation guarantees the performance of organizations, departments, or individuals [28].

There is some research into the CSFs of IA implementation in organizations. Bunker [29] states that organizational business strategies and strategic directions affect IA. The Qatari Ministry of Information and Communications Technology (MICT) states that the main factors to protect information are education for employee and user awareness since they are the managers and users of the information [30].

Cherdantseva and Hilton [11] describe the security countermeasures in the implementation of security and IA; these are focused on human-oriented, legal, technical, and organizational aspects. CESG, which is a group within the GCHQ, published "The Information Assurance Maturity Model and Assessment Framework" [57]. The main IA process goals are governance and leadership; awareness, education, and training; compliance; assured information sharing; through-life IA measures; and information risk management. Chris Cope suggested principles for enhancing organizational security. These principles strongly emphasize a risk-driven and holistic approach, business alignment, and adequate governance in an environment less constrained by policies [31].

Additionally, it seems that multiple factors are a challenge in e-Government service implementation in addition to IA, such as cultural issues, digital divide, and trust issues [32]–[34]. Moreover, alongside these factors, security, coordination, and infrastructure also affect Indonesian IA implementation [35]–[37]. Such a challenge is tackled in the suggested framework to assure the continuation of Indonesian e-Government services.

C. The Proposed Framework

The proposed framework has its basis in desk research and was expanded upon in the last research paper [38]. The framework is composed of three categories, as shown in Fig. 1.

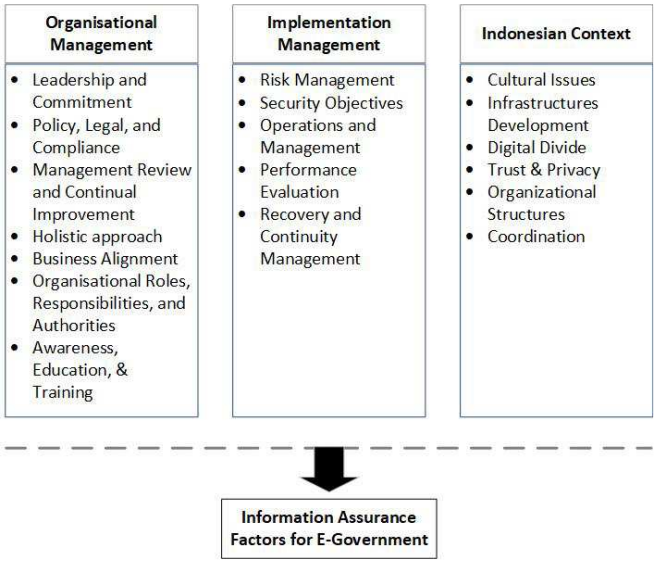

Fig. 1 Information assurance framework for e-government in Indonesia

The framework is divided into three categories based on the scope and meaning. The importance and justification of the chosen factors are elaborated as follows:

1) Organizational Management: The subsequent factors are related to organizational management in e-Government IA implementation within the Indonesian context.

- Leadership and Commitment (OF1). Leadership and commitment from the highest organizational level in IA implementation are vital for achieving IA through to the initial planning [58]. Top management needs to make sure that IA objectives and policies are in line with the needs of the business. Additionally, the required resource availability needs to be guaranteed [9].
- Policy, Legal, and Compliance (OF2). The policy guides the IA to be congruent with business needs (IASME). The legal team must make sure that there are legal guarantees for information use, intellectual property rights, and product and software use [11]. Moreover, organizations must ensure information system compliance with standards and policies [30].
- Management Review and Continual Improvement (OF3). Senior management must conduct periodic reviews of continual effectiveness, adequacy, and suitability of the IA policy [9]. The reviews could show the necessity of constant improvement for the suitability, competence, and effectiveness of the IA policy [9].
- Holistic Approach (OF4). The IA is a combination of technical, personnel, procedural, and physical security [31]. Furthermore, IA is not only a technology issue, as the majority of threats are from humans. The holistic treatment of IA defenses are multi-layered, and a weakness in one aspect can also be covered in other aspects [12].
- Business Alignment (OF5). Practically, security and IT are not independent of each other, but both support the business [39]. The IA must accommodate business needs [29]. Because businesses run on risk, through IA planning, focusing on business aims, risks are kept

to a minimum, and organizations' information is guaranteed [31].

- Organizational Roles, Responsibilities, and Authorities (OF6). Senior management must assign organizational roles within the organization [30]. The top management also needs to ensure responsibilities and authorities to confirm that IA affirms with standards [9].
- Awareness, Education, and Training (OF7). People working in organizations must be aware of IA policies and how they contribute to IA performance and effectiveness, as well as the implications if they fail to comply with IA requirements [9]. Furthermore, every employee must receive education and training regarding their job function [30]. Also, every employee should be competent in their field [27].

2) Implementation Management: The following factors are linked to implementation management e-Government IA implementation in the Indonesian context.

- *Risk Management (IF1).* The first stage of risk management is asset enumeration and planning; this calculates and categorizes the assets owned by the organization [9]. Additionally, the process plans the use of organizational assets. These are identified as defining the overall information asset risk from the assessment results [26]. The results show that risk treatments are to be determined. The risk may not be eradicated but can be kept to a minimum [9].
- *Security Objectives (IF2).* Information security goals need to be pertinent to the functions as well as levels of the information security policy [9]. Furthermore, when determining information security requirements and security objectives, the risk assessment and treatment results need to be taken into consideration.
- Operations and Management (IF3). Organizations need to guarantee the planning, implementation, and control are compliant with the requirements of information security [9]. To guarantee optimum security, security systems must be updated according to the latest provider updates [26].
- Performance Evaluation (IF4). Performance evaluation comprises internal audit, monitoring, evaluation, analysis, and measurements. Internal audit will confirm if the IA implementation complies with IA policy and organizational needs [9]. Information regarding IA implementation effectiveness and maintenance is also gathered from the audit results. Further, measurement, monitoring, inquiry, and evaluation affect the effectiveness and performance of the IA implementation [26].
- Recovery and Continuity Management (IF5). Backup and restore maintaining information system integrity and availability during disasters or incidents [9]. If a major information system failure occurs, the continuation of the business must be ensured and functioning as normal [26].

3) Indonesian Context: The challenges and factors in implementing e-Government and IA in Indonesia, in addition to those in other developing countries, are presented as follows.

- Cultural Issues (CF1). Cultural issues must be taken into consideration during IA implementation [26]. This is akin to the cultural issues influencing organizational behaviors in Indonesia that influence IA implementation [32]–[34].
- Infrastructure Development (CF2). E-Government implementation needs improved system infrastructure to provide services as planned [26]. Additionally, infrastructure is also required for the achievement of information security processes in regard to security goals [40]. Developing countries such as Indonesia usually find it difficult to develop basic infrastructures (Anggono, Hardjaloka).
- Digital Divide (CF3). Differences in geography, ethnicity, race, as well as a class in developing countries, particularly Indonesia, bring about gaps in accessing technology, notably the Internet [40]. This must be addressed in regard to IA implementation, especially as a less developed region still may not have achieved its objectives.
- Trust and Privacy (CF4). For e-Government implementation to be achieved, there should be trust amongst citizens and government [40]. Given the large quantities of users' information to be controlled in regard to information privacy, the government should protect user information [40].
- Organizational Structures (CF5). The creation of a national-scale organization such as the National Cyber Agency for handling issues of information security is necessary [22]. This organization oversees other organizations which exist in the management of government information security issues, including e-Government [35].
- Coordination (CF6). In several Indonesian government institutions, coordination is needed amongst institutions so that institutional duties do not cross over into the protection of e-Government services [35], [37].

D. Research Method

The triangulation method was selected and applied in this research. The reason to choose the triangulation method is derived from the purpose of this research. The present research is intended to examine, review, and confirm the factors for IA framework for e-Government in Indonesia. Further, the triangulation method is able to combine the qualitative method, which is useful in obtaining the differentiated opinions of the results, and the quantitative method, which is used to test them. The method incorporates the strength of each method and is aimed at increasing the validity and testing the hypotheses [41].

The qualitative method aims at describing and analyzing phenomena to get new information and helps to discover new theoretical insights [41], [42]. A qualitative approach is related to data in the form of beliefs, perceptions, opinions, or ideas that are not easily shown in numbers. Methods for collecting data in a qualitative approach include interviews, observations, focus groups, and document analysis [42], [43].

The quantitative method is frequently used to confirm previously developed hypotheses and it involves the data collection, analysis, and interpretation that can be expressed

in numbers [41], [42]. A common way for data collection in the quantitative approach is by questionnaire [42]. The main benefit of the questionnaire is that it can be used to collect data from a massive number of respondents [59]. A questionnaire consists of a set of questions to gather responses from participants. To record the answers from respondents in a questionnaire, a scale is commonly used [45].

The triangulation method consists of three phases. The first phase in this research was the literature review, which was presented in sub-section A in section 2 and was aimed to identify the IA framework factors. The second phase was the expert interviews that aimed to review and receive experts' opinions on the proposed IA framework. The final phase was the survey of practitioners in Indonesia, which aimed at confirming the proposed framework. Fig.2 illustrates the triangulation method for this study.

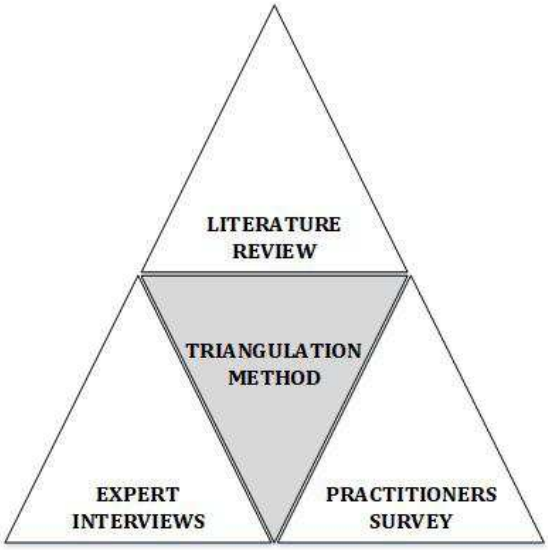

Fig. 2 Triangulation method to confirm the proposed framework

1) Expert Interviews

Expert sampling was used since the interviews were targeted at obtaining experts' opinions. Using expert sampling, subjects are selected based on their expertise or knowledge [46]. The sample size relies upon saturation, where there is no more knowledge which is able to be collected [47]. Romney et al. [48] stated that in qualitative interviews, respondents who are expert on the topic reached saturation with around 4-5 respondents. Furthermore, there is a Discounted Expert Review Theory which 75% of usability comes from three to five experts, after that it reaches saturation [49]. Therefore, taking errors into account, the sample study size was 8 experts evaluating the framework validity. A pre-test for testing the interview questions was conducted with three people, one was a security expert and two were from government agencies.

The qualitative interviews were aimed at reviewing the developed framework. The developed framework was reviewed by conducting interviews with IA, information security, and e-Government experts in Indonesia with at least five years of experience. Interviews were conducted in Indonesia. Interview questions were in the form of semi-structured and consisted of close-ended as well as open-ended questions. There were 18 closed-ended which were intended to obtain expert feedback on the current factors in the proposed framework. The open-ended part was aimed to explore more information other than factors that already identified.

2) Practitioners Survey

An online questionnaire was sent to IA, information security, and e-Government practitioners from Indonesia government agencies, universities, and research institutes in different locations around Indonesia. The questionnaire had a total of 46 items, which consisted of 18 factors that are derived from three categories, as explained in detail in [38].

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) [50]. 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 [51]. 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 [51]. A pre-test survey was conducted with five experienced practitioners from government agencies, universities, and researchers in Indonesia.

To determine the sample size, the central limit theorem states that, as the sample size increases, which is usually designated as bigger than 30, the sampling distribution will be normally distributed despite the shape of the population from which the sample was picked [52]. Moreover, the margin of error must be [53]. Two error types 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 determine the sample size required for the study.

For this, the statistical power analysis program, G* Power, was used to determine the minimum sample size [54], which resulted in 23 minimum sample size. For this research, the minimum sample size was decided at 30. The reason for this number was that the sample size of 30 covered both the calculation from the statistical power analysis program and the central limit theorem. Furthermore, in this study, the Cronbach's Alpha was used for guaranteeing the item reliability and effectively measure the factors.

III. Results and Discussion

This section presents the results and discusses the confirmed IA framework for e-Government in Indonesia. To confirm the framework, a mixed-methods approach that combines the qualitative and quantitative approaches was used. Expert interviews were conducted as a process to review the factors that had been identified. While practitioners survey conducted to confirm the factors that have been reviewed.

A. Findings from the Expert Interviews

Further, the objective of the open-ended questions in expert interviews is to get broad analysis and review for identifying other factors about IA implementation for e-Government in Indonesia. A thematic analysis was conducted to analyze the data. The analysis started with a process of encoding information that produced a theme list, which is an approach that seizes something significant concerning the data in relation to the research question that portrays a pattern in responses [55]. This was intended to be able to organize, systemize data in a complete and detailed so that data can bring up a picture of the topics being studied. The importance of the proposed factors, according to the experts' insights are highlighted as followed**:**

1) Organizational Management

- Leadership and Commitment. All experts reported the critical importance of leadership and commitment in the implementation of IA for eGovernment in Indonesia, as Expert 4 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".

- 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 Expert 8:

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

  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, organizations must comply with the policy and legal aspects that have been established, as stated by Expert 7:

  "Policy and legal aspects are essential for implementation to work out. In addition, organizations are required to comply with the policies and legal aspects".

- 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 Expert 2:

  "It is important to review policies. But in practice, the management review in government organizations is not undertaken by the board level. The board will usually appoint senior management to review and then report to the board".

- Holistic Approach. All experts supported the significant importance of a 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 Expert 8:

  "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 of the implementation of IA".

- Business Alignment. All experts reported the importance of business alignment in the implementation of IA for eGovernment in Indonesia, as Expert 1 stated:

  "Alignment of IA with the business is important, and to achieve it, an organization must pay attention to business needs, understand subject matters, suitable assessment, criteria and assess".

- Organizational Roles, Responsibilities, and Authorities. All experts supported the importance of organizational roles, responsibilities, and authorities in the implementation of IA for eGovernment in Indonesia, as stated by Expert 1:

  "The one responsible for determining the direction of the organization 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 organization has its roles, responsibilities, and authorities".

2) Implementation Management

- Awareness, Education, and Training. All experts supported the significant importance of awareness, education, and training in the implementation of IA for eGovernment in Indonesia. This factor is important in the implementation, as stated by two 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).

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

- Risk Management. All experts agreed on the importance of risk management in the IA implementation for eGovernment in Indonesia, as stated by Expert 5:

  "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, organizations are ready to handle the risks".

- Security Objectives. All experts reported the importance of security objectives in the

implementation of IA for eGovernment in Indonesia, as Expert 7 stated:

"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".

- 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 following the plan, as stated by Expert 2:

  "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".

- 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 Expert 1:

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

- 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 Expert 3:

  "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".

3) Indonesian Context

- 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 organization, as stated by an expert:

  "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 the habits of the people in Indonesia. So cultural issues are influential" (Expert 8).

- Infrastructures Development. All experts reported the critical importance of infrastructure development in the implementation of IA for eGovernment in Indonesia, as Expert 5 stated:

  "Infrastructures are important in supporting the implementation of IA. Although infrastructure 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".

- 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 the geographical location that is not reached by technological developments, as stated by Expert 2:

  "If for example, the central government wants to implement into each region, the 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 they can become a bottleneck".

- 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 can 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 Expert 8 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 by the party who is not authorized or misused. It could be mined and exploited by others".

- Organizational Structures. All experts supported the importance of organizational 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 Expert 6:

  "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 the National Cyber and Crypto Agency is to function as an agency that overshadows and coordinate other agencies".

- 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 Expert 4:

"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".

The analysis from the results of the expert interviews [60] shows, despite one expert, is disagreed on the Recovery and Continuity Management, it can be said that all experts are agreed that the rest of the factors are important for the implementation of IA for e-Government in Indonesia. Hence, from the analysis, it can be concluded that all the factors are significant.

B. Results of the Questionnaires

This section part provides the survey results. Quantitative data was obtained via online questionnaires. A total of 32 practitioners responded and filled out the questionnaire. Every respondent is an Indonesian practitioner operating in information assurance, information security, or an e-Government field with over 2 years' experience. The objective of the survey is to confirm the suggested framework. Closed questions refined the framework factors. The closed-ended questions involved forty-six items, where one to six was stating each of the factors. A four-point Likert Scale was used. One Sample T-test analyzed the quantitative data.

The test enables the assessment of mean value distribution. The hypothesized mean (μ_0) and test value were designated as 2.5. The hypotheses for the testing of each of the factors are as follows:

- H_0: There is no statistically significant difference between the mean factor and the equivalent of its null value
- H_1: There is a statistically significant difference between the mean element and the equivalent of its null value

TABLE I
DESCRIPTIVE ANALYSIS FOR QUESTIONNAIRE RESULTS

Factors	N	Minimum	Maximum	Mean	Std. Deviation
OF1	32	3.00	4.00	3.77	0.38
OF2	32	3.00	4.00	3.66	0.48
OF3	32	2.50	4.00	3.42	0.46
OF4	32	3.00	4.00	3.66	0.48
OF5	32	3.00	4.00	3.69	0.47
OF6	32	3.00	4.00	3.44	0.50
OF7	32	3.00	4.00	3.63	0.46
IF1	32	3.00	4.00	3.72	0.46
IF2	32	3.00	4.00	3.48	0.43
IF3	32	3.00	4.00	3.50	0.44
IF4	32	3.00	4.00	3.53	0.51
IF5	32	3.00	4.00	3.72	0.38
CF1	32	2.00	4.00	3.64	0.541
CF2	32	3.00	4.00	3.63	0.44
CF3	32	2.00	4.00	3.56	0.52
CF4	32	3.00	4.00	3.53	0.51
CF5	32	2.00	4.00	3.45	0.56
CF6	32	3.00	4.00	3.66	0.48

To analyze the answers given by participants, descriptive analysis was used to understand the responses, it involves summarizing and organizing the data so they can be easily understood. Table 1 shows the descriptive analysis of the results.

Furthermore, the hypothesis was tested for each requirement using a non-parametric statistical test. This test is a test whose model does not specify conditions regarding the parameters of the population from which the sample was drawn. For this test, a one-sample median test as an alternative to t-test [56], the Wilcoxon signed-rank test, is used to test whether a sample median differs significantly from a hypothesized value. In this test, the median value is 2.5 since this number falls on the 'Disagree' before the 'Agree' point on the four-point Likert scale.

Moreover, the statistically significant level alpha (α) is 0.05. It means the null hypothesis (H_0) is rejected if the probability (p-value) < α = 0.05. If a factor has a p-value < 0.05, then the factor is statistically, as else the factor is not statistically significant. Further, in this study, the Bonferroni correction was used to control false positive findings through dividing alpha (α= 0.05) by the number of questionnaire items (46). The p-value that has been adjusted is 0.001.

Note that a confidence level of 95% was used to conduct the hypothesis test. Table 2 illustrates the questionnaire result analyses for each of the factors.

TABLE II
ONE SAMPLE MEDIAN TEST: WILCOXON SIGNED RANK TEST OF QUESTIONNAIRE RESULTS

Category	Median Value = 2.5		
	Items	Sig	Decision
Organizational Management	OF1	<0.001	Reject the null hypothesis
	OF2	<0.001	Reject the null hypothesis
	OF3	<0.001	Reject the null hypothesis
	OF4	<0.001	Reject the null hypothesis
	OF5	<0.001	Reject the null hypothesis
	OF6	<0.001	Reject the null hypothesis
	OF7	<0.001	Reject the null hypothesis
Implementation Management	IF1	<0.001	Reject the null hypothesis
	IF2	<0.001	Reject the null hypothesis
	IF3	<0.001	Reject the null hypothesis
	IF4	<0.001	Reject the null hypothesis
	IF5	<0.001	Reject the null hypothesis
Indonesian Context	CF1	<0.001	Reject the null hypothesis
	CF2	<0.001	Reject the null hypothesis
	CF3	<0.001	Reject the null hypothesis
	CF4	<0.001	Reject the null hypothesis
	CF5	<0.001	Reject the null hypothesis
	CF6	<0.001	Reject the null hypothesis

From the results, every item shows a mean >2.5 and p-value <0.001, thus, H_0 is rejected and the H_1 is accepted. Thus, it can be concluded that all category attitudes and factors show significance in influencing the implementation of IA.

Furthermore, in this study, the Cronbach's Alpha was used for guaranteeing the item reliability and effectively measure the factors. To conduct the Cronbach's Alpha test SPSS software was used. Table 3 provides a summary of the reliability test of the factors.

TABLE III
RELIABILITY TEST OF QUESTIONNAIRE RESULTS

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.938	0.939	46

The overall result of Cronbach's Alpha reliability test of factors is 0.938. Bryman and Cramer [61] stated that a Cronbach's alpha of approximately 0.7 means that the internal consistency of items measured is good, whilst the internal consistency of approximately 0.8 or greater is very good. Therefore, it can be said that the results of the items in Table 3 are reliable.

IV. CONCLUSION

The goal of the research is to construct a framework for information assurance to assist in the implementation of e-Government in Indonesian. In order to achieve an effective IA implementation, it is important to identify factors that can affect the implementation. The proposed framework was constructed by identifying factors from industry standards that recognized internationally, international publications of relevant literature, and challenges of IA and e-Government in the Indonesian context. The framework comprises of 18 factors and classified into three categories. To validate the proposed framework, it was then reviewed and confirmed in two phases.

The first phase was reviewing the factors that had been identified and explored other factors by conducting interviews with eight experts from various institutions 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. The second phase, which was aimed to confirm the reviewed framework, involved a survey that was distributed to IA, e-Government, information security practitioners in Indonesia. The results indicated that all factors are statistically significant.

The framework will be used in future studies as a reference to develop an instrument to asses IA implementation for e-Government in Indonesia. Moreover, the results from the full study 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.

REFERENCES

[1] World Bank, "Technology & Development," *Global Economic Prospects 2008: Technology Diffusion in the Developing World*, 2008.

[2] V. Ndou, "E-Government for Developing Countries: Opportunities and Challenges," *EJISDC Electron. J. Inf. Syst. Dev. Ctries.*, vol. 18, no. 1, pp. 1–24, 2004.

[3] H. Wang and B. L. Rubin, "Embedding e-finance in e-government: a new e-government framework," *Electron. Gov. an Int. J.*, vol. 1, no. 4, pp. 362–373, 2004.

[4] S. Cohen and W. Eimicke, "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)*, 2002, vol. 5, no. January, p. 146b (1-10).

[5] I. S. Sipatuhar and Sutaryo, "Faktor-Faktor Penentu Implementasi E-Government Pemerintah Daerah di Indonesia," *Simp. Nas. Akunt. XIX*, pp. 24–27, 2016.

[6] Presiden Republik Indonesia, "Kebijakan dan Strategi Nasional Pengembangan E-Government," *Instruksi Presiden Republik Indonesia Nomor 3 Tahun 2003*. 2003.

[7] P. T. Jaeger and K. M. Thompson, "E-government around the world: Lessons, challenges, and future directions," *Gov. Inf. Q.*, vol. 20, no. 4, pp. 389–394, 2003.

[8] S. Basu, "E-government and developing countries: an overview," *Int. Rev. Law, Comput. Technol.*, vol. 18, no. 1, pp. 109–132, 2004.

[9] ISO/IEC 27001, "ISO/IEC 27001:2013," no. September 2014, 2015.

[10] E. A. Hibbard, *Introduction to Information Assurance*. 2009.

[11] Y. Cherdantseva and J. Hilton, "A Reference Model of Information Assurance & Security," *Proc. 8th ARES Conf. 2013 (ARES 2013)*, pp. 1–11, 2013.

[12] C. J. May, J. Hammerstein, J. Mattson, and K. Rush, "Defense in Depth: Foundation for Secure and Resilient IT Enterprises," 2006.

[13] A. Rathmell, S. Daman, K. O'Brien, and A. Anhal, "Engaging the Board Corporate Governance and Information Assurance," 2004.

[14] A. M. Rugman and S. Collinson, "International Culture," *Int. Bus.*, pp. 129–158, 2006.

[15] R. Schware, *E-development from excitement to effectiveness*. 2005.

[16] Z. Fang, "E-Government in Digital Era : Concept , Practice , and Development," vol. 10, no. 2, pp. 1–22, 2002.

[17] CNSS, "National Information Assurance Glossary," *CNSS Instr. No. 4009*, vol. CNSSI No., no. 4009, 2010.

[18] P. Liu, M. Yu, and J. Jing, "Information Assurance," *Handb. Inf. Secur. Inf. Warf. Soc. Leg. Int. Issues Secur. Found. Vol. 2*, 2006.

[19] C. Lambrinoudakis, S. Gritzalis, F. Dridi, and G. Pernul, "Security requirements for e-government services: A methodological approach for developing a common PKI-based security policy," *Comput. Commun.*, vol. 26, no. 16 SPEC., pp. 1873–1883, 2003.

[20] S. Alfawaz, L. May, and K. Mohanak, "E-government security in developing countries : A managerial conceptual framework," *Inf. Syst. Manag.*, no. March, pp. 26–28, 2007.

[21] P. Upadhyaya, S. Shakya, and M. Pokharel, "Security Framework for E-Government Implementation in Nepal," *J. Emerg. Trends Comput. Inf. Sci.*, vol. 3, no. 7, pp. 1074–1078, 2012.

[22] F. Setiadi, Y. G. Sucahyo, and Z. A. Hasibuan, "Balanced E-Govemment 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*, 2013.

[23] T. K. Priyambodo and Y. Prayudi, "Information security strategy on mobile device based egovernment," *ARPN J. Eng. Appl. Sci.*, vol. 10, no. 2, pp. 652–660, 2015.

[24] S. Wang and Y. Sun, "Research on information security assurance system of E-government," *Proc. - 2009 Int. Conf. Comput. Intell. Softw. Eng. CiSE 2009*, 2009.

[25] G. Karokola, S. Kowalski, and L. Yngström, "Secure e-Government Services: Towards A Framework for Integrating IT Security Services into e-Government Maturity Models," in *Information Security South Africa (ISSA) 2011*, 2011.

[26] D. A. Booth, *The Standard for Information Assurance for Small and Medium Sized (IASME)*, no. 2.3. The IASME Consortium Ltd and David A. Booth 2013, 2013.

[27] ISACA, *COBIT 5 for Assurance*. Rolling Meadows, IL 60008 USA: ISACA, 2013.

[28] C. V. Bullen and J. F. Rockart, "A primer on critical success factors," *Work. Pap.*, no. 69, pp. 1–64, 1981.

[29] G. Bunker, "Technology is not enough: Taking a holistic view for information assurance," *Inf. Secur. Tech. Rep.*, vol. 17, no. 1–2, pp. 19–25, 2012.

[30] MICT, *National Information Assurance Policy 2.0*, no. 2.0. 2014., 2014.

[31] C. Cope, "10 Principles for Effective Information Assurance," 2015.

[32] D. A. Wicaksono, “E-Government in Indonesia : the Opportunities and Challenges,” *Development*, pp. 1–2, 2003.
[33] J. S. Djumadal, “Implementasi E-Government, Sebuah Harapan Penuh Tantangan Di Provinsi Daerah Istimewa Yogyakarta,” in *Konferensi dan Temu Nasional Teknologi Informasi dan Komunikasi untuk Indonesia*, 2008.
[34] L. Hardjaloka, “Studi Penerapan E-Government di Indonesia dan Negara Lainnya Sebagai Solusi Pemberantasan Korupsi di Sektor Publik,” *RechtsVinding*, vol. 3, no. 3, 2014.
[35] H. Ardiyanti, “Cyber-security dan tantangan pengembangannya di indonesia,” *Politica*, vol. 5, no. dinamika masalah politik dalam negeri dan hubungan internaisonal, pp. 95–110, 2014.
[36] B. D. Anggono, “E-Government Indonesia: Strategi Penyelenggaraan Data Center Pemerintah Indonesia,” 2015.
[37] L. Operananta, “Cyber security: Indonesia’s Challenges and Opportunities to move forward.” 2015.
[38] R. G. Utomo, R. J. Walters, and G. B. Wills, “Factors affecting the implementation of information assurance for eGovernment in Indonesia,” in *2017 12th International Conference for Internet Technology and Secured Transactions, ICITST 2017*, 2018.
[39] R. Burge, “Lincolnshire Police Information Assurance Strategy, Standards and Working Practices,” no. June, p. 59, 2014.
[40] M. A. Khalil, B. D. Lanvin, and V. Chaudhry, “The E-Government Handbook for Developing Countries,” *AProject InfoDev Cent. Democr. Technol.*, no. November, 2002.
[41] V. Venkatesh and S. A. Brown, “Bridging the Qualitative–Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems,” *MIS Q. Vol. X No. X, pp. 1-XX/Forthcoming 2012–2013*, vol. X, no. X, pp. 1–34, 2013.
[42] J. Recker, *Scientific research in information systems: a beginner's guide. Springer Science & Business Media*, 2012.
[43] C. Anderson, “Presenting and evaluating qualitative research,” *Am. J. Pharm. Educ.*, vol. 74, no. 8, 2010.
[44] J. Lazar and J. Preece, “Social considerations in online communities: Usability, sociability, and success factors,” *Cogn. Digit. world*, no. October, pp. 1–46, 2002.
[45] M. Saunders, P. Lewis and A. Thornhill, *Research Methods for Business Students*. Pearson, New York., 2009.
[46] A.. Bhattacherjee, *Social Science Research: principles, methods, and practices*, vol. 9. 2012.
[47] G. Guest, A. Bunce, and L. Johnson, “How Many Interviews Are Enough?,” *Field methods*, vol. 18, no. 1, pp. 59–82, 2006.
[48] A. K. Romney, S. C. Weller, and W. H. Batchelder, “Culture as Consensus: A Theory of Culture and Informant Accuracy,” *Am. Anthropol.*, vol. 88, no. 2, pp. 313–338, 1986.
[49] Y. Rogers, H. Sharp, and J. Preece. *Interaction Design: Beyond Human-Computer Interaction*. Wiley., 2011.
[50] R. Garland, “The mid-point on a rating scale: Is it desirable?,” *Res. Note 3*, vol. 2, pp. 66–70, 1991.
[51] Y. Cherdantseva, “Secure * BPMN - a graphical extension for BPMN 2 . 0 based on a Reference Model of Information Assurance & Security,” no. December, 2014.
[52] A. Field, *Discovering Statistics Using SPSS*, vol. 81, no. 1. 2013.
[53] A. Banerjee, U. Chitnis, S. Jadhav, J. Bhawalkar and S. Chaudhury, "Hypothesis testing, type I and type II errors", *Industrial Psychiatry Journal*, vol. 18, no. 2, p. 127, 2009. Available: 10.4103/0972-6748.62274.
[54] F. Faul, E. Erdfelder, A. Buchner, and A.-G. Lang, “Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses,” *Behav. Res. Methods*, vol. 41, no. 4, pp. 1149–1160, 2009.
[55] V. Braun and V. Clarke, “Using thematic analysis in psychology,” *Qual. Res. Psychol.*, vol. 3, no. 2, pp. 77–101, 2006.
[56] 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.
[57] CESG, “The Information Assurance Maturity Model and Assessment Framework,” no. 2.1, 2015.
[58] C. Tannahill, “Information Assurance Strategy NHS Lanarkshire,” no. 4, 2013.
[59] Lazar, J., & Preece, J., 2002. Social considerations in online communities: Usability, sociability, and success factors.
[60] 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.
[61] A. Bryman, “Qualitative Data Analysis Qualitative Data,” *Soc. Res. methods*, pp. 564–589, 2012.