Framework Index security information to support evaluation, adoption and improvement of methods in developing variables

Framework Index security information to support evaluation, adoption and improvement of methods in developing variables

F M Kaffah[1,*], C Slamet[1], A B A Rahman[2], K Manaf[3] and B Subaeki[4]

[1] Department of Information System, Informatics and Business Faculty, UIN Sunan Gunung Djati, Bandung, Indonesia
[2] Department of Information Communication Technology AEU, Malaysia
[3] Department of Information System, Sangga Buana YPKP University Bandung, Indonesia
[4] Department of Informatics Engineering, Sangga Buana YPKP University Bandung, Indonesia

*faiz@uinsgd.ac.id

Abstract. The governance of information security in the Indonesian Government has not been completely improved. Many related variables components are not measured. This study aims to observe an evaluation for application of information security index framework in Indonesian government institutions as the implementation of electronic government. The analysis is carried out by adopting an information security index framework produced in the rank of e-government. The study uses a triangulation approach within a mixed method. This study results in a novel adoption model of information security index framework equipped by two new variables. Therefore, a proper policy of the Indonesian government is required for its implementation.

1. Introduction

Along with the very fast development in the digital economy, the government simultaneously tries to implement an information technology which is assumed to change the service model, reduce the costs and time that usually occurs in paper-based administrative models. Besides that, the government continuously tries to increase the active participation the of the community in achieving the goals of the State [1]. Based on the report issued by ID-SIRTII in 2015, Indonesia does not have sufficient policies and strategies related to cybersecurity [2]. Symantec Information Security Threat Report Usage Report, Indonesia's overall global ranking for coding from 7th rank in 2014 to rank 5th in 2015 [3]. This was due to Indonesia's increasing economic growth and manufacturing is one of the main drivers of Indonesia's GDP growth in 2015 [4].

E-government or electronic government is the use of information technology by the government to provide information and services to its citizens, both in matters related to government and business and business. The importance of e-government is based on the transparent needs of the government and the demands of changing times. The program certainly has a purpose, one of which is to improve public services through the use of information and communication technology.

2. Literature review

Electronic administration (e-adm) is an electronic substitution expression given to a government that adopts the internet-based technology, an intranet that can complement and improve its programs and services. The main goal is to provide the best satisfaction to service users or to provide maximum satisfaction [5]. Information security governance is the formation and maintenance of a controlled environment to manage risks related to confidentiality, integrity, and availability (CIA) and supporting processes and systems [6]. The World Bank views e-government as an adoption of the development of the utilization of global banking technology. The development of e-gov is intended to improve the efficiency, effectiveness, transparency, and accountability of government management by using the internet and other digital technologies [7,8].

Information security is an attempt to secure information assets against threats that may arise. So that information security can indirectly guarantee business continuity, reduce risks that occur, optimize return on investment (return on investment) [9,10].

In reference, the comparative analysis of the Information Security Governance Framework: Public Sector Approach, proposes 9 frameworks for information security governance for the public sector such as A practical guide to implementing and controlling Information Technology Security Governance, Business Software Alliance, Information security policy: An organizational- process model level, Information Technology Security Governance (Von Solms,2007), COBIT, ISO / IEC Standards, ITGI, NIST, and Software Engineering Institute [11-13].

3. Methodology

This methodology contains the results of interviews involving two government officials who are authorized to determine the regulation. The first is a consultant from the Indonesian Security Incident Response Team on the Internet Infrastructure (ID-SIRTII) which is an institution to handle or respond to cybercrime incidents that occurred in Indonesia. The second is from the Ministry of Communication and Information (MENKOMINFO) which is authorized to carry out the duties of the law and make government regulations. This methodology is described in the form of questions that refer to the following three criteria:

- Q1: What is the basis for the Information Security Index Regulation
- Q2: What security methods can be applied in the implementation of these regulations
- Q3: What are the factors that have caused a security system leak in Indonesia

Next is to prepare data to be designed as a form of description of a case obtained from the interview. During this process, we can obtain phenomena that can be described in the form of classification, identification, categories that will be linked to the data obtained from the results of previous interviews. So that, in the end, we can get an interpretation in conclusion.

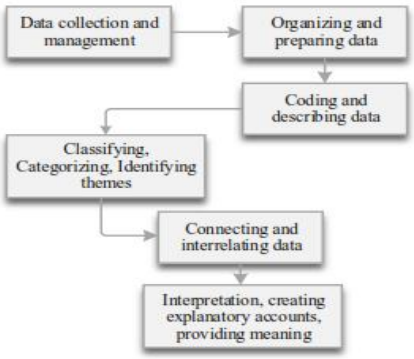

Figure 1. Data analysis technique.

This study uses a socio-technical approach in the process of obtaining data, especially those relating to the security of e-government information technology in Indonesia. This section contains comparative analysis that is most relevant to the governance of information security in the public sector described earlier. The absence of a standard framework for comparing types of information security governance frameworks so that it uses a set of criteria from various fields of research that the author obtained in the previous reference. These criteria were chosen by considering various types of information security governance frameworks in the existing public sector such as Government Government Criteria, Governance Criteria, Security Criteria and Public Sector Suitability

4. Result and discussion

In the results and discussions that are carried out, there can be an architectural model. This is a description that explains how the maturity of the model can be applied in government management. Data quality is the main factor that can be part of the socio-technical approach in this research method. Data accuracy is also a factor that can be a risk in the mistake of implementing regulations made by the government. As well as facts in law enforcement that are lacking in handling a particular case.

The impact that can occur if government management, especially those related to information technology security, is data leakage and misuse of these data. Renewal in technology is also a very complex factor in influencing government policy and also the lack of experts in working as professionals is a major factor in making information security safeguarded.

The policies made by the government, in general, are closely related to management, regulation, institutions, and technology. How to get the maturity value is determined from the relevant application stage category. Each question section has a different application stage category. How to get the maturity value is determined from the sum of the question scores based on the application category starting from the largest category. The maturity level of the information security management process, the extension of completeness evaluation and used to identify the level of maturity of the application of security with categories that refer to the maturity level used in the information security index standard framework.

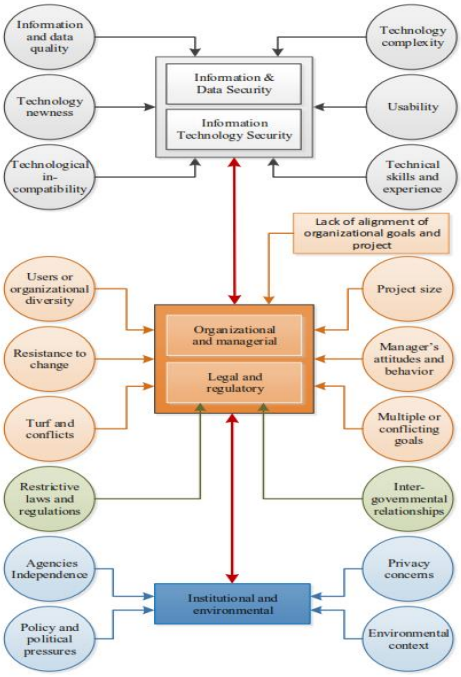

Figure 2. Purpose framework index security.

5. Conclusion

The development of this readiness model is basically to determine how much the government is doing in implementing an information security system in government management. This effort is carried out as an alternative for stakeholders in determining the direction of their policies. Very rapid technological renewal, lack of law enforcement and lack of resources, especially professionals who work in implementing national information security systems. Also, support from all relevant elements is needed in maintaining national security, especially in information technology security issues in government management portals.

References

[1] Power R 2002 *CSI/FBI computer crime and security survey*
[2] Syakhroza A 2003 Best Practices Corporate Governance dalam Konteks Kondisi Lokal Perbankan Indonesia *Usahawan* **32** 6 13–20
[3] ISO 2008 ISO/IEC 27001:2005 - Information technology — Security techniques — Information security management systems — Requirements Technologies *Inf. Syst.* 34
[4] Standard I 2005 *INTERNATIONAL STANDARD ISO / IEC 27002 — Code of practice for information security management* Iso 27002
[5] Informasi T D K 2011 *Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik* **2** 1
[6] Gehrmann M 2012 Combining ITIL , COBIT and ISO / IEC 27002 for structuring comprehensive information technology for management in organizations *Navus - Rev. Gest. e Tecnol.* **2** 66–77
[7] Clinch J 2009 ITIL v3 and information security *Clinch Consult. White Pap.* 1–40
[8] Irfan M, Zulfikar W B, Alam C N, D S Maylawati and Fuadi R 2018 Conceptual Model of xecutive Information System Data (A CaseStudy at The State Islamic University of Sunan Gunung jati Bandung) *IOP Conf. Ser. Mater. Sci. Eng.* 105
[9] Knapp K J, Franklin Morris R, Marshall T E and Byrd T A 2009 Information security policy: An organizational-level process model *Comput. Secur.* **28** 7 493–508
[10] Irfan M Readiness of information technology *J. Online Inform.* **1** 1
[11] Van Bon J, Pieper M, van der Veen A and Verheijen T 2008 *Foundation of IT Service Management based on ITIL* (Van Haren Publishing)
[12] ISACA 2007 CoBIT 4.1 *IT Gov. Inst.* 1–29
[13] Calder A and Watkins S 2008 *IT governance : a manager's guide to data security and ISO 27001/ISO 27002* (Kogan Page Ltd.)