InComTech: Jurnal Telekomunikasi dan Komputer
vol.12, no.3, Desember 2022, 204-217
http://publikasi.mercubuana.ac.id/index.php/Incomtech
P-ISSN: 2085-4811 E-ISSN: 2579-6089

Strategy for Implementation of the Security Maturity Model in e-Government Systems in Indonesia

Tashia Indah Nastiti*

Informatics Engineering, Faculty of Engineering and Computer Science, Indraprasta PGRI University
Jl. Nangka Raya No.58 C, South Jakarta, Indonesia
*Corresponding Email: tashiaindah.unindra@gmail.com

Abstract:
To determine the current status of security implementations and to plan overall security system improvements, the security maturity level of Indonesia's e-government system must be evaluated. Generally, the maturity model describes how a system consisting of humans and devices performs its duties. These capabilities include effective leadership and governance, the level of awareness of implementers, and the capabilities of existing tools. This study aims to create a strategy for implementing the security maturity model in the e-Government system in Indonesia. The research method uses a mixed method, namely qualitative and quantitative methods. The qualitative approach aims to obtain the Critical Success Factors (CSF) implementation of the security maturity model. The quantitative method is used to analyze the Critical success factor validation results using SPSS. The strategy for the security maturity model is based on the PDCA (Plan-Do-Check-Act) model.

***Key Words**:*
Security;
Maturity Model;
PDCA;
Framework;
Assessment

Article history:
Received March 29th, 2022
Revised July 16th, 2022
Accepted July 25th, 2022
Published December 26th, 2022

DOI:
10.22441/incomtech.v12i3.15214

1. INTRODUCTION

The Government of Indonesia developed and implemented an e-Government system in all government sectors in 2003, following Presidential Instruction No. 3 of 2003 concerning National Policy and Strategy for e-Government Development. However, in its adaptation, the security aspect is often not prioritized during the development and use of the system, affecting the service's continuity and resulting in the loss of critical and personal information. Although the Indonesian government has pushed for a safe system for all government agencies by issuing different laws, policies, and guidelines regarding the implementation of information

security, only a few e-Government systems that fully follow these documents create E-Systems as safe government.

The evaluation of the security of Indonesia's e-Government system should be carried out to find out the current situation of security implementation in the system and to ensure the continuity of the system by planning improvements for the implementation of security for the system. The maturity model is considered one of the standard tools in performance evaluation, and the term "maturity" has been used in various areas and disciplines. The term's definition also depends on the context in which it is used [1]. According to Nobert Frick et al. (2013), in their research, the maturity model is a tool for assessing the effectiveness of an organization in achieving increasingly organized and systematic governance in the organization [2]. The maturity model consists of five "maturity levels," from lowest to highest, namely initial, managed, defined, quantitatively managed, and optimization (however, the number of levels may vary depending on the domain and model variation) [1]. This maturity model technique supports organizations as (1) measures for auditing and benchmarking; (2) measurement of progress assessment against objectives; and (3) an understanding of the strengths, weaknesses, and opportunities (which can support decision making regarding the project management strategy and portfolio).

Several references are related to maturity models that already exist globally, such as PRISMA, C2M2, ISO 27002: 2013, ISM3, and the US Index [3]. Strategy can minimize the occurrence of subjectivity in the evaluation results of security maturity. Therefore, this study aims to obtain a strategy for implementing the security maturity model so that the results of the model are objective and comparable among government agencies.

2. METHODOLOGY

The methodology is a guide, method, and sequence of work used in this study. Apart from that, the methodology determines the expected output of each step. The research methodology's purpose is to make the process more efficient. In addition, the method is expected to make it easier to monitor research progress and success rates. Figure 1 shows the research methodology used in this study.

2.1 Research Problem

To identify problems in this study, the Kitchenham method is used in this study. Kitchenham's method collects problems from previous studies [4]. From this stage, it can be seen that there are problems related to the inappropriate use of the cybersecurity maturity model in several ministries in Indonesia. Improperly used security maturity models can result in subjective, non-transparent, and incomplete assessments. This is because not all security maturity models can be used by all sectors and have clear assessment procedures. Therefore, this study has two research questions, namely:

1. What are the success factors for implementing the security maturity model?
2. What is the strategy for implementing the security maturity model?

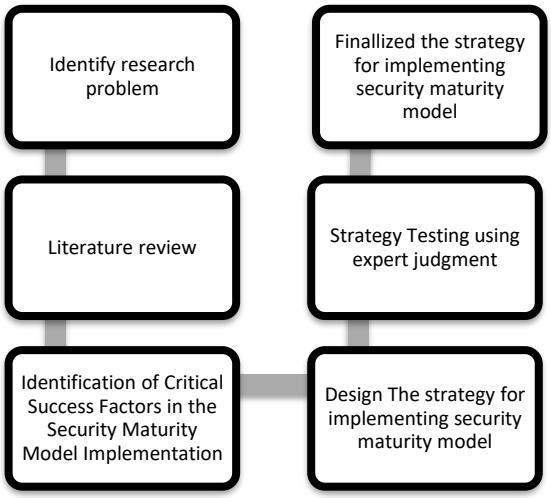

Figure 1. Research Methodology

2.2 Literature Review

In the literature review stage, researchers used the snowballing method. Snowballing refers to using a reference list of a paper or citations to identify additional papers [5]. However, snowballing can benefit from seeing a list of references or citations and knowing where articles are being referred to or cited. Using references and quotes can be done with backward snowballing and forward snowballing. Snowballing guidelines are illustrated and evaluated by replicating a published reliability study of a systematic literature review.

At this stage, the researcher compared the existing e-government security maturity models. The models used are C2M2, PRISMA, ISM3, KAMI Index, ISO 27002: 2013, and PeGI. Researchers used the taxonomy method adapted from the research of Angel Marcelo Rea-Guaman et al. (2017) to determine comparison categories [6]. This comparison category is used as the basis for developing strategies for using the security maturity model, so validation must be carried out using a research instrument in the form of a questionnaire. The taxonomy consists of general, process, organization, and quality.

This comparison of security maturity models is carried out to see the different use characteristics and assessments of each existing security maturity model. It can be easier to determine the appropriate security maturity model for use in government agencies in Indonesia. From comparisons, the authors conclude that the KAMI Index is the proper model for use in government agencies in Indonesia. The KAMI Index is a model designed to assess security systems in government agencies that has continuity and is regularly updated according to current technological advances.

According to the State Intelligence Agency's head of the technology department, the KAMI Index makes a significant contribution to the realization of information security in government agencies, both central and regional, BUMN, and companies or other organizations. It is hoped that the KAMI Index can encourage and improve security in government agencies in strategic sectors.

2.3 Identification of Critical Success Factors in the Security Maturity Model Implementation

Critical Success Factors (CSF) are critical factors that significantly affect the success of a project. CSF is closely related to a goal. Goals are targets created to achieve the mission of an organization, company, or project, while CSFs are factors that must be appropriately controlled so that these goals can be achieved [7].

At this stage, identifying success factors in implementing the security maturity model is carried out through various studies using Kitchenham's theory. Kitchenham et al. (2019) provide research techniques for analyzing state-of-the-art knowledge by formally presenting problem formulas, information sources, search strings, criteria for entering or issuing problems, qualitative analysis, and templates for reporting from the information collected [4]. Using the Kitchenham theory will make it easier for researchers to get relevant data and interpret it according to CSFs.

Articles or papers submitted from the IEEE and the Science Direct Database from 2010 to 2019, the study must have 2 (two) main focuses, namely the Security Maturity Model and Critical Success Factors of Security Maturity Models Implementation. The study must also comply with the established criteria for inclusion, namely: (1) Paper on security maturity model implementation (2) Complete and published paper (3) Paper in English.

These CSFs will then be validated to determine the significance of each success factor using a questionnaire distributed later to several experts and respondents.

2.4 Designing a Strategy Using the Plan-Do-Check-Act Model

The implementation strategy theory used to develop a strategy for implementing the security maturity model is the PDCA model [8]. The PDCA model consists of four steps:

1) Plan: The plan category has points that affect the successful implementation of the security maturity model. An example is determining the competence of the assessment team.
2) Do: The Do category has points that affect the success of data collection, observation, and documentation.
3) Check: The Check category has influence points when analyzing results and assessments using the security maturity model.
4) Act: The Act category has a point that affects the outcome and ongoing treatment of deficiencies in aspects of the security maturity model.

2.5 Strategy Testing

The strategy testing for implementing the security maturity model is carried out using the expert judgment method. Expert judgment is used to complete, validate, interpret, and integrate available data; assess the impact of changes that occur on the organization; predict future events and the consequences of each decision; determine the current state; and provide the elements needed for the proper decision-making process [9].

The success factor items compiled into a strategic design are then validated by the experts in the form of a questionnaire using the validity and reliability test. Validity is a measure that indicates that the variable being measured is the variable to be studied [10]. A test can be said to have high validity if it performs its measurement function or provides precise and accurate measurement results following the test's purpose. Using more than one factor means testing the item's validity by correlating the item score with the factor score, then proceeding to correlate the item score with the total factor score (sum of several factors). From the results of these calculations, a correlation coefficient will be obtained, which is used to measure an item's validity level and determine whether an item is feasible to use. In determining whether an item will be used, a correlation coefficient significance test is usually carried out at a significance level of 0.05, meaning that an item is considered valid if it correlates significantly with the total score. The Pearson bivariate correlation (Pearson moment product) is a testing technique that researchers frequently use to assess validity. This analysis is done by correlating the score of each item with the total score. The sum of all items yields the total score. Question items that are significantly correlated with the total score indicate that the item can provide support in expressing what is desired. Legitimate. If r is calculated rtable (2-sided test with sig. 0.05), then the instrument or item correlates significantly with the total score (declared valid).

Reliability is an index that shows the extent to which a measuring instrument can be trusted or reliable. A measuring tool is considered dependable if it is used repeatedly to assess the same symptoms and the measurement findings are largely consistent. In other words, dependability demonstrates how consistently a measuring tool measures a certain symptom. Reliability shows how the results of measurements made with these tools can be trusted. The measurement results must be reliable because they must have consistency and stability. High and low reliability are empirically indicated by a number called the reliability coefficient value. High reliability is indicated by the rxx value being close to 1. The general agreement is that reliability is considered satisfactory at 0.700. Testing the instrument's reliability using the Cronbach alpha formula is necessary because this research instrument is in the form of a questionnaire and a graded scale [11]. The validity and reliability of this instrument can be tested using the SPSS program. Items from the strategy that are not eliminated will be used to implement the security maturity model

3. RESULT AND DISCUSSION

This section explains the results of the research and, at the same time, provides a comprehensive discussion.

3.1. Identification of Success Factors in Implementing the Maturity Model

Success factors for implementing the security maturity model were identified using the Kitchenham method. Each success factor listed in Table 1 is supported by several concepts in and across studies where all the existing success factors have the same level of importance. It means that nothing is more or less important. To support the successful implementation of the security maturity model, the government and other relevant parties must pay attention to the generated success

factors. However, in the next section, all of these success factors become input for the success factor validation process so that the success factors generated in this study are valid and reliable.

Table 1. Critical Success Factor

No	Item (Critical Success Factor)	Article
1	Get physical and technical evidence	[12]
2	Conduct regular assessments	[12]
3	Determine the vision, mission, and requirements for the implementation of the security maturity model	[6], [13]
4	Prepare a supporting application	[2], [14]
5	Active communication	[14], [15]
6	Forming an assessment team	[15], [16]
7	Get access to all information systems	[15], [17]
8	Configure, test, and troubleshoot	[15], [18]
9	Monitor and evaluate assessor performance	[15]
10	Manage data exchange	[12], [15]
11	Determine budget, and implementation time	[15]
12	Provide education to the evaluation target	[18], [19]
13	Collecting respondents following the evaluated field	[19]
14	Get leadership support	[20]
15	Ensure the completeness of documents	[20], [21]
16	Determining the competency of the assessment team	[21], [22]
17	Identify the resources needed to carry out the evaluation	[23]
18	Defining maturity planning	[23]
19	Knowledge of Security Maturity Model	[24]
20	Designing an evaluation scheme	[24]

3.2. Design Security Maturity Model Implementation Strategy

The design of the security maturity model implementation strategy is based on validated success factors that have been previously tested. The strategy's design using the Plan-Do-Check-Act (PDCA) model is divided into four parts as shown in Table 2.

3.3. Strategy Testing

Furthermore, the design of the strategy will be tested again to obtain a valid strategy. In this second iteration, the strategy items will be tested using the expert judgment method on 48 experts as respondents.

Table 2. Security Maturity Model Implementation Strategy

Plan	Determine the vision, mission, and requirements for the implementation of the security maturity model
	Setting up support applications
	Forming an assessment team
	Determine budget, and implementation time
	Get leadership support
	Determining the competency of the assessment team
	Identify the resources needed to carry out the evaluation
	Defining maturity planning
	Knowledge of Security Maturity Model
	Designing an evaluation scheme
Do	Effective communication
	Have access to all information systems
	Configure, test, and troubleshoot
	Manage data exchange
	Collecting respondents following the evaluated field
	Provide education to the evaluation target
Check	Have physical and technical evidence
	Monitor and evaluate rater performance
	Ensure completeness of documents
Act	Conduct regular assessments

3.3.1. Respondent's Demography

Respondents to this study were employees, staff, or officials in government agencies in charge of technology and information. In collecting test data, 48 respondents were successful. The following is the respondents' demographic data, which contains positions and agencies.

Respondent's agency data from the 48 respondents who filled out the most questionnaires came from the State Intelligence Agency, namely, 24 respondents (50%). Then, Indosat has nine respondents (19%). The Ministry of Home Affairs has five respondents (11%). The Ministry of Political, Legal, and Security Affairs and PT Telkom had 4 respondents (8%). The Ministry of Defense has two respondents (4%).

The State Intelligence Agency, the Ministry of Home Affairs, the Ministry of Defense, PT Indosat Ooredo, and PT Telkom are agencies or companies with a high security urgency level. The VP Head of the Cyber Security Operation Center stated that Indosat Ooredo has confidential data, and if a leak occurs, it will significantly impact the company and the customer. Like the State Intelligence Agency, the Head of the Sub-Directorate at the Deputy for Technology stated that the State Intelligence Agency has information that is not for public consumption and requires strict permission to obtain it. Meanwhile, the Coordinating Ministry for Political,

Legal, and Security Affairs is an agency with a moderate urgency for information security because its data does not contain strict confidentiality.

From the 48 respondents who were collected, 22 respondents or 46% were staff, 10 respondents or 21% were analysts, eight respondents or 17% were directors or managers (Echelon II), as many as 6 respondents or 12% were heads of subdivisions (Echelon IV), and as many as 2 respondents or 4% are department heads (Echelon III).

Echelon II and Echelon III are officials who have the authority to make decisions and provide their views as decision-makers. Meanwhile, Echelon IV, Analysts, and Staff are field implementers who understand the organization's conditions and facts in order to provide views as field implementers.

3.3.2. Expert's Interview

After conducting interviews with three sources, the demographics of the speakers can be seen in Table 3 as follows.

Table 3. Interviewee Demography

Interviewee	Occupation	Institution	Degree
Interviewee 1	VP Head of Cyber Security Operation Center	Indosat	Strata – 2
Interviewee 2	Head of Section at Deputy for Technology	Indonesian State Intelligence Agency	Strata – 2
Interviewee 3	Head of Sub-Directorate at the Deputy for Technology	Indonesian State Intelligence Agency	Strata – 2

The interview results show that information security in an organization is a critical and significant concern. A security maturity model is an important tool in evaluating security and developing security systems, especially in government agencies. However, not all government agencies and organizations have implemented the security maturity model (KAMI Index) as a security evaluation tool.

This security maturity model is expected to assess various areas or aspects of security, especially in governance, processes, human resources, and technology. The governance area can correct some weaknesses in the governance management system to significantly impact information security system management. At the same time, processes and resources are highly interrelated factors where the process will work best if people with good knowledge drive it. Information system security is closely related to technological advances owned by agencies/organizations, so technology is an important area that must be considered by agencies and organizations.

In implementing the security maturity model, it is necessary to have a clear strategy because it can simplify the control and monitoring process of all activities, whether they follow the rules or strategy. The strategy is expected to provide clear stages, from selecting the assessment team to evaluating evaluation reports such as CMMI and COBIT.

3.3.3. Analysis of Data

In this study, the agreement of the experts on each item in the form of a success factor in the implementation of the security maturity model was tested for content validity and homogeneity reliability with the Aiken's V approach. As previously mentioned, content validity was estimated by testing the test content's feasibility or relevance through rational analysis by a competent panel or expert judgment.

1) Reliability Test of Success Factors for Implementation of Security Maturity Model

At this stage, the homogeneity reliability coefficient will be calculated for each success factor item using the Aiken's H formula that has been given, so that the results are as shown in Table 4. Based on the homogeneity reliability significance standard (H), for 48 people, the number of experts (raters). Moreover, with 5 categories (Likert scale), the minimum homogeneity reliability coefficient (H), which is considered significant, is 0.51 (H > 0.51) [25]. Thus, the 20 items will be tested for their level of reliability using the homogeneity of reliability (H) indicators as follows:

Table 4. Homogeneity Reliability (H) of Items

PDCA	Item (Critical Success Factor)	V Coefficient
Plan	Determine the vision, mission, and requirements for the implementation of the security maturity model	0.931
	Setting up support applications	0.931
	Forming an assessment team	0.928
	Determine budget, and implementation time	0.928
	Top Management Support	0.925
	Determining the competency of the assessment team	0.927
	Identify the resources needed to carry out the evaluation	0.932
	Defining maturity planning	0.924
	Knowledge of Security Maturity Model	0.925
	Designing an evaluation scheme	0.932
Do	Effective communication	0.928
	Have access to all information systems	0.929
	Configure, test, and troubleshoot	0.924
	Manage data exchange	0.926
	Collecting respondents following the evaluated field	0.928
	Provide education to the evaluation target	0.931
Check	Have physical and technical evidence	0.925
	Monitor and evaluate rater performance	0.925
	Ensure completeness of documents	0.925
Act	Conduct regular assessments	0.925

Based on the coefficient values of the results in the table above, it can be seen that all items have a coefficient value of > 0.51. Therefore, it can be said that the

20 items have appropriate content validity and good homogeneity reliability. Thus, no item is excluded from the list of success factors.

2) Validity Test

Data analysis was carried out to test the involvement of at least 48 experts, who were very useful for assessing the content contained in the instrument [26]. The instrument, which contained 20 items of success factors using a Likert scale, was distributed to 48 experts in the field of expert judgment.

In other words, several experts were asked for their level of agreement on whether each item of the implementation strategy for the implementation of the security maturity model followed the opinion of the expert until an agreement was reached. The questionnaire instrument was created using a Likert scale from 1 to 5, with 1 indicating "strongly disagree," 2 indicating "disagree," 3 indicating "neutral," 4 indicating "agree," and 5 indicating "strongly agree." All 48 experts filled out the questionnaire that had been distributed, and even in this questionnaire, some experts added or proposed additional success factors. However, the added success factors have been accommodated by the existing ones. The first stage is calculating the content-validity coefficient for each success factor item using Aiken's V formula so that it is obtained as shown in Table 4.

Based on the standard of content validity (V), for 48 experts (raters) and 5 categories (Likert scale), the minimum content validity coefficient (V) that is considered significant is 0.70 (V > 0.50). The first stage is to calculate the content-validity coefficient for each success factor item using Aiken's V formula to obtain it, as shown in Table 5. Based on the content validity significance standard (V), for 48 people, the number of experts (raters), and 5 categories (Likert scale), the minimum content validity coefficient (V), which is considered significant, is 0.50 (V > 0.50).

At this stage, all 20 newly synthesized concepts are the items of the strategy for implementing the security maturity model, which can be expressed as presented in Table 5. As seen in Table 5, the value of the content validity coefficient (V) of each success factor ranges from 0.376 to 0.785. However, there are 5 items of success factors (marked in gray) that do not meet the significant standard (V<0.50), so the 5 items of the strategy must be removed from the implementation strategy of the security maturity model. This means that the 5 items of the strategy have no significant effect on the implementation strategy of the security maturity model.

3.3. Security Maturity Model Implementation Strategy

Based on the study results, 15 items were found to be significant for use in the security maturity model strategy. The following Table 6 is a strategy for implementing the security maturity model using the PDCA model. The strategy for implementing the security maturity model is divided into three main stages: which are: Plan, Do, Check, and Act. In Plan stages, there are six points that must be considered in implementing the security maturity model: forming an assessment team, determining budget and implementation time, top management support, determining the competency of the assessment team, defining maturity planning, and knowledge of the security maturity model.

Tabel 5. Content Validity (V) of Items

PDCA	Item (Critical Success Factor)	V Coefficient
Plan	Determine the vision, mission, and requirements for the implementation of the security maturity model	0.392
	Setting up support applications	0.387
	Forming an assessment team	0.599
	Determine budget, and implementation time	0.590
	Top Management Support	0.749
	Determining the competency of the assessment team	0.657
	Identify the resources needed to carry out the evaluation	0.421
	Defining maturity planning	0.758
	Knowledge of Security Maturity Model	0.749
	Designing an evaluation scheme	0.474
Do	Effective communication	0.594
	Have access to all information systems	0.540
	Configure, test, and troubleshoot	0.785
	Manage data exchange	0.713
	Collecting respondents following the evaluated field	0.603
	Provide education to the evaluation target	0.443
Check	Have physical and technical evidence	0.753
	Monitor and evaluate rater performance	0. 713
	Ensure completeness of documents	0.742
Act	Conduct regular assessments	0.735

In Do stage, there are five points that must be considered in implementing the security maturity model: effective communication, access to all information systems, configuration, testing, and troubleshooting, managing data exchange, and collecting respondents following the evaluated field.

In Check stage, there are three points that must be considered in implementing the security maturity model: having physical and technical evidence, monitoring and evaluating rater performance, and ensuring the completeness of documents. The final stage is Act, which has only one point to consider: conducting regular assessments.

Table 6. Security Maturity Model Implementation Strategy

Plan	Forming an assessment team
	Determine budget, and implementation time
	Top Management Support
	Determining the competency of the assessment team
	Defining maturity planning
	Knowledge of Security Maturity Model
Do	Effective communication
	Have access to all information systems
	Configure, test, and troubleshoot
	Manage data exchange
	Collecting respondents following the evaluated field
Check	Have physical and technical evidence
	Monitor and evaluate rater performance
	Ensure completeness of documents
Act	Conduct regular assessments

4. CONCLUSION

The security maturity model framework is needed to minimize subjectivity in the evaluation results of security maturity. The security maturity model framework is created using the PDCA model. Based on strategy validity testing, the value of the content validity coefficient (V) of each success factor ranges from 0.376 to 0.785. Thus, there are 5 items of success factors that do not meet the significant standard (V<0.50), so those 5 of the 20 strategy items must be removed from the implementation strategy of the security maturity model.

The framework is divided into four parts. The Plan consists of forming an assessment team, determining the budget and implementation time, getting leadership support, determining the competence of the assessment team, defining the maturity plan, knowledge about the security maturity model. Then, Do consists of effective communication, has access to the entire information system, performs configuration, tests, troubleshoots, manages data exchange, and collects respondents according to the evaluated areas. Check consists of having physical and technical evidence, monitoring and evaluating the assessor's performance, and ensuring the documents' completeness. Finally, the Act consists of conducting periodic assessments.

REFERENCES

[1] D. I. Sensuse, A. Nasbey, Nordianto, R. Dewiyanti, R. Novira, and M. F. Dzulfikar, "PeGI in practice: The e-government assessment in National Library of Indonesia," *2017 5th Int. Conf. Cyber IT Serv. Manag. CITSM 2017*, 2017, doi: 10.1109/CITSM.2017.8089296.

[2] N. Frick, T. F. Küttner, and P. Schubert, "Assessment methodology for a maturity model for interorganizational systems - The search for an assessment procedure," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, pp. 274–283, 2013, doi: 10.1109/HICSS.2013.106.

[3] Z. Yunos, R. Ahmad, and M. Yusoff, "Grounding the component of cyber terrorism framework using the grounded theory," *Proc. 2014 Sci. Inf. Conf. SAI 2014*, pp. 523–529, 2014, doi:

10.1109/SAI.2014.6918237.

[4] M. K. Najafabadi and M. N. Mahrin, "A systematic literature review on the state of research and practice of collaborative filtering technique and implicit feedback," *Artif. Intell. Rev.*, vol. 45, no. 2, pp. 167–201, 2015, doi: 10.1007/s10462-015-9443-9.

[5] C. Wohlin, "Guidelines for Snowballing in Systematic Literature Studies and a Replication in Software Engineering," *18th Int. Conf. Eval. Assess. Softw. Eng. (EASE 2014)*, pp. 1–10, 2014, doi: 10.1145/2601248.2601268.

[6] A. M. Rea-Guaman, T. S. Feliu, J. A. Calvo-Manzano, and I. D. Sanchez-Garcia, "Comparative Study of Cybersecurity Capability Maturity Models," *Int. Conf. ...*, vol. 1, no. November, pp. 30–42, 2017, doi: 10.1007/978-3-319-67383-7.

[7] P. Rahayu and D. I. Sensuse, "CSF for implementation e-portfolio model: A Systematic Review," *2015 Int. Conf. Inf. Technol. Syst. Innov. ICITSI 2015 - Proc.*, 2016, doi: 10.1109/ICITSI.2015.7437714.

[8] M. Meng, "The research and application of the risk evaluation and management of information security based on AHP method and PDCA method," *2013 6th Int. Conf. Inf. Manag. Innov. Manag. Ind. Eng.*, pp. 379–383, 2013.

[9] C. J. Torrecilla-Salinas, O. De Troyer, M. J. Escalona, and M. Mejías, "A Delphi-based expert judgment method applied to the validation of a mature Agile framework for Web development projects," *Inf. Technol. Manag.*, vol. 20, no. 1, Mar. 2019, doi: 10.1007/s10799-018-0290-7.

[10] W. Techataweewan and U. Prasertsin, "Development of digital literacy indicators for Thai undergraduate students using mixed method research," *Kasetsart J. Soc. Sci.*, vol. 39, no. 2, pp. 215–221, 2018, doi: 10.1016/j.kjss.2017.07.001.

[11] Sugiyono, *Quantitative, Qualitative, and R&D Research Methods*. Bandung: Alfabeta, 2015.

[12] D. Lie and M. Satyanarayanan, "Quantifying the Strength of Security Systems," *Proc. 2Nd USENIX Work. Hot Top. Secur.*, pp. 3:1--3:6, 2007, [Online]. Available: http://dl.acm.org/citation.cfm?id=1361419.1361422

[13] F. Setiadi, P. H. Putra, Y. G. Sucahyo, and Z. A. Hasibuan, "Determining components of national cyber security framework using Grounded Theory," *Proc. 2nd Int. Conf. Informatics Comput. ICIC 2017*, vol. 2018-Janua, pp. 1–6, 2018, doi: 10.1109/IAC.2017.8280637.

[14] F. Setiadi, Y. G. Sucahyo, and Z. A. Hasibuan, "Balanced E-Government security framework: An integrated approach to protect information and application," *Proc. 2013 Int. Conf. Technol. Informatics, Manag. Eng. Environ. TIME-E 2013*, pp. 95–98, 2013, doi: 10.1109/TIME-E.2013.6611971.

[15] J. M. Denolf, J. H. Trienekens, P. M. Wognum, J. G. A. J. Van Der Vorst, and S. W. F. Omta, "Towards a framework of critical success factors for implementing supply chain information systems," *Comput. Ind.*, vol. 68, pp. 16–26, 2015, doi: 10.1016/j.compind.2014.12.012.

[16] B. Borgman, S. Mubarak, and K. K. R. Choo, "Cyber security readiness in the South Australian Government," *Comput. Stand. Interfaces*, vol. 37, no. 2015, pp. 1–8, 2015, doi: 10.1016/j.csi.2014.06.002.

[17] P. Upadhyaya, S. Shakya, and M. Pokharel, "E-government security readiness assessment for developing countries: Case study: Nepal Govt. organizations," *Asian Himalayas Int. Conf. Internet*, pp. 1–5, 2012, doi: 10.1109/AHICI.2012.6408453.

[18] F. Ghaffari and A. Arabsorkhi, "A New Adaptive Cyber-security Capability Maturity Model," *9th Int. Symp. Telecommun. With Emphas. Inf. Commun. Technol. IST 2018*, pp. 298–304, 2019, doi: 10.1109/ISTEL.2018.8661018.

[19] V. Swarnakar, A. R. Singh, J. Antony, A. Kr Tiwari, E. Cudney, and S. Furterer, "A multiple integrated approach for modelling critical success factors in sustainable LSS implementation," *Comput. Ind. Eng.*, vol. 150, no. August, p. 106865, 2020, doi: 10.1016/j.cie.2020.106865.

[20] M. Rizal and Y. G. Sucahyo, "A study on the preparedness of information security framework area based on the assessment of information security index in Ministry of XYZ," *2013 Int. Conf. Adv. Comput. Sci. Inf. Syst. ICACSIS 2013*, no. March, pp. 55–59, 2013, doi: 10.1109/ICACSIS.2013.6761552.

[21] L. Adedayo, S. Butakov, R. Ruhl, and D. Lindskog, "E-Government web services and security of Personally Identifiable Information in developing nations a case of some Nigerian embassies," *2013 8th Int. Conf. Internet Technol. Secur. Trans. ICITST 2013*, pp. 623–629, 2013, doi: 10.1109/ICITST.2013.6750278.

[22] D. I. Sensuse, M. Syarif, H. Suprapto, R. Wirawan, D. Satria, and Y. Normandia, "Information

security evaluation using KAMI index for security improvement in BMKG," *2017 5th Int. Conf. Cyber IT Serv. Manag. CITSM 2017*, 2017, doi: 10.1109/CITSM.2017.8089293.

[23] R. M. Adler, "A dynamic capability maturity model for improving cyber security," *2013 IEEE Int. Conf. Technol. Homel. Secur. HST 2013*, pp. 230–235, 2013, doi: 10.1109/THS.2013.6699005.

[24] L. Hakim and A. Tarigan, "Using the Information Security Index to Measure University Information Security Management : Concepts and Strategies," vol. 4, no. 5, pp. 1623–1635, 2018.

[25] N. Feng and M. Li, "An information systems security risk assessment model under uncertain environment," *Appl. Soft Comput.*, vol. 11, no. 7, pp. 4332–4340, 2011, doi: 10.1016/j.asoc.2010.06.005.

[26] A. D. Stivala, J. H. Koskinen, D. A. Rolls, P. Wang, and G. L. Robins, "Snowball sampling for estimating exponential random graph models for large networks," *Soc. Networks*, vol. 47, pp. 167–188, 2016, doi: 10.1016/j.socnet.2015.11.003.