Information Security Maturity Model

A Best Practice Driven Approach to PCI DSS Compliance

Semi Yulianto
Information Technology Department
Swiss German University, BSD City,
Tangerang 15339, Indonesia
semi.yulianto@student.sgu.ac.id

Charles Lim
Information Technology Department
Swiss German University, BSD City,
Tangerang 15339, Indonesia
charles.lim@sgu.ac.id

Benfano Soewito
Master of Information Technology
Bina Nusantara University
Jakarta 11530, Indonesia
benfano@gmail.com

***Abstract*— A successful of PCI DSS implementation depends on the capability of the organization's information security in providing the effective safeguard of their information asset, while cardholder data security is the main concern. Many organizations failed to comply with the standard, and this eventually results in fines or even termination of the ability to process credit cards. Clearly, an evaluation mechanism or tool used to measure the current state of the organization's information security is needed. In this paper, an Information Security Maturity Model for PCI DSS (ISMM-PCI) with four maturity level - None, Initial, Basic and Capable - was proposed. The ISMM-PCI utilizes the use of quantitative and qualitative analysis, enhancing the PCI DSS to ISO/IEC 27001 mapping, and focuses on improving the quality of people, process and technology. The model assists the organizations to easily identify the key success factors and gaps (point of weaknesses), provides the guideline to better manage information security and formulate the best strategy for the enhancement, improving the overall information security state by selecting the best security countermeasures (controls) to protect their information assets from the emerging cyber-attacks, while achieving PCI DSS full compliant. The main advantage of ISMM-PCI over other ISMMs is its ease of use. The comparative analysis of the case results affirms the statement. ISMM-PCI may be used by a wide range of organizations regardless of the size.**

Keywords*— *PCI, PCI DSS, ISO/IEC 27001, compliance, compliant, maturity, model.

I. INTRODUCTION

The Payment Card Industry Data Security Standard (PCI DSS) also known as PCI Security Standards is an information security standard for any organization that handles cardholder information of the leading credit card providers such as American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Data security is the primary concern of PCI DSS, defined in their data security compliance programs. Any organization that stores, processes or transmits cardholder data is required to comply with PCI DSS requirements [14][15]. PCI DSS presents best security practices that can be adopted as the common-sense steps to protect the overall information asset. PCI DSS does not only contain the 12 (twelve) high-level requirements to be satisfied but also contain information security best practices which must be adopted and applied to any merchants and payment card processors. PCI security is expected to be the vital result of the adopted framework. The essence of PCI compliance relies on three steps: assess, remediate and report.

A successful information security program, standard or framework aims to safeguard the information assets is driven by people, supported by a proper documentation of the process which includes formalized policies, procedures, and guidelines. Many organizations focused on enhancing technology without paying more attention to reviewing, improving, and enhancing the current processes, and forgetting the human element of the information technology itself (people).

The current implementation approach does not allow organizations to satisfy the 12 (twelve) high-level requirements set by PCI DSS effectively. Most organizations failed to satisfy the minimum required security controls in order to secure data while transmitting (data in motion), processing (data in process), and storing (data at rest) sensitive and confidential cardholder data. The possible "scope creep" and organization's incapability also increase the chance of possible delay and even failure to comply with PCI DSS at the required level. Possible weaknesses and other affecting factors (internal and external) should be identified soonest possible at the earliest stage of the PCI DSS implementation in order to avoid or not to waste time, cost, and effort as well as putting the business at risk.

PCI DSS compliant is definitely the main goal besides improving and maintaining the overall information security state of the organizations. Dominant factors affecting compliance achievement should be evaluated to identify the key success factors as well as the most common gaps in meeting the requirements. Clearly, an evaluation mechanism or tool used to measure the current state of the organization's information security is needed. The expected mechanism should be simple, reliable, easy to use, and utilizes the industry best practices while providing a clear roadmap followed by the best strategy, not only to comply with PCI DSS, but advancing the overall information security state of the organization as

978-1-5090-0931-2/16/$31.00 ©2016 IEEE

well as to protect their information assets from the emerging cyber-attacks.

The proposed maturity model suggests a mechanism to properly measure the organizations' information security capability to comply with PCI DSS, select proper controls, and come up with the best strategy presented as strategic options according to their maturity levels. The model considers several information security maturity models which were analyzed to be adopted or based on the Systems Security Engineering Capability Maturity Models (SE-CMM, 2003) which appears to give better foundation and understanding in developing or building a security maturity model. Information security management, evaluation, and awareness are the three major categories found in most of the models [9]. Based on the nature of the mechanism to be used along with with PCI DSS compliance evaluation, the model will be called "Information Security Maturity Model for PCI DSS" (ISMM-PCI). The model allows the organizations to evaluate the information security capability against the industry standards and frameworks in the form of best practices approach.

Following are the organization of the paper: Section II summarizes the related works, Section III discusses our proposed model, Section IV describes our model evaluation and Section V presents model validation, Section VI summarizes and concludes our research findings.

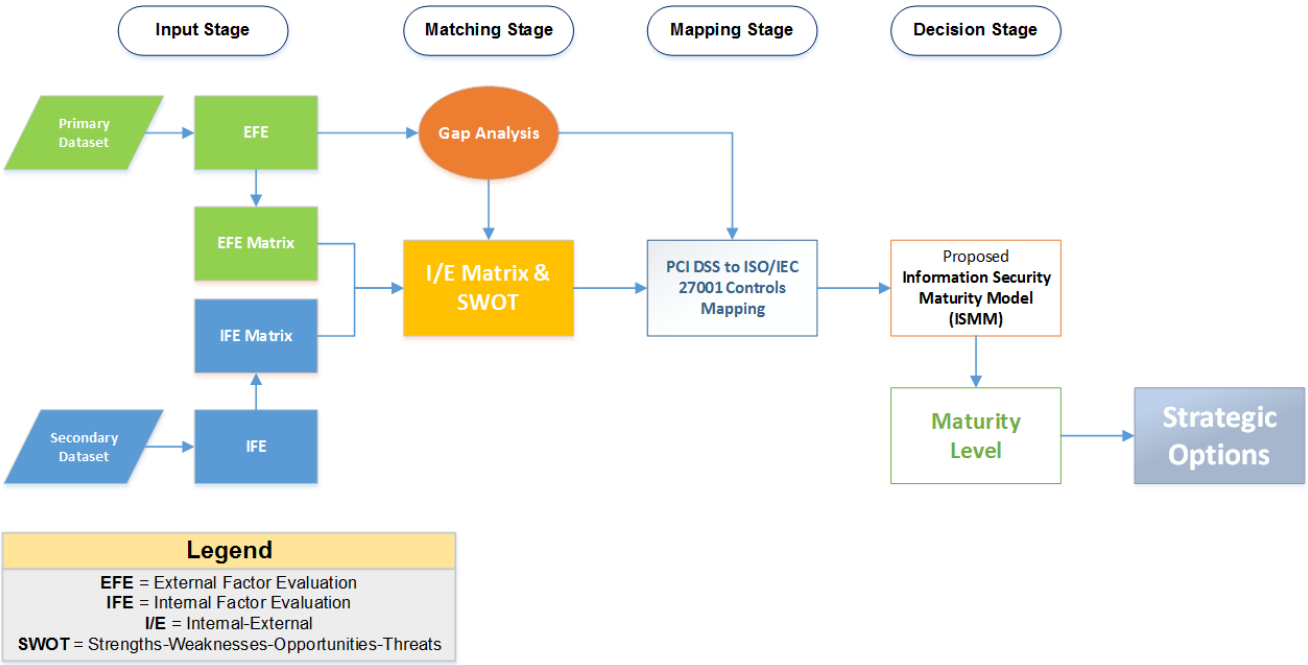

Fig. 1. Model Development Framework

II. Related Works

Past works by several researchers [4][9][10][11][13][18] mostly focused on the critical analysis based on literature review. Considering the work of Matrane [13] and Karokola [9], case study supported by quantitative and/or qualitative analysis were not utilized in order to justify the veracity and the effectiveness of the proposed models. The studies were based on literature review and theoretical proposals without supporting case study on applying the model to the actual real-world scenarios. Yet, no method of measurement of the current state of security and related processes were presented.

This study focuses on measuring the initial maturity level of targeted organizations in order to satisfy the twelve high-level PCI DSS requirements. It considers the study of Saleh [18] with regards to the domains mapped to implementation standards and levels of compliance. Additionally, this study utilizes the use of quantitative and qualitative analysis based on different data collection instruments, enhancing the PCI DSS to ISO/IEC 27001 mapping [12][16][17][19] and focuses on quality of people, process, and technology. It presents a practical approach to effectively identify the key success factors as well as the most common gaps in the PCI DSS compliance requirements and adhere to the continuous advancement of information security, in the form of a universal and comprehensive information security model applicable to a wide range of organizations and industries, regardless of size. Additionally, best practice driven information security governance model presented by Lessing [11] were utilized and enhanced.

III. Information Security Maturity Model

The development of ISMM-PCI model involved in evaluating several factors gathered at the input stage, processed at the matching stage, and use the results at the decision stage. The Input Stage takes the input from several factors such as internal and external evaluation translated in

the form of the matrix (IFE & EFE). The Matching Stage takes the input of the Strength-Weaknesses-Opportunities-Threats (SWOT) and combined it with the Internal-External (IE) matrix to get the expected maturity level and detect or identify point of weaknesses prior to getting the Strategic Options. The Mapping Stage takes the input from the Matching Stage, map PCI DSS requirements to ISO/IEC 27001:2013 controls with the objective to generalize specific PCI DSS requirements into controls. The Decision Stage takes the input from the Mapping Stage, use the proposed Information Security Maturity Model (ISMM), analyze the results, and finally decide the best strategy or approach. Fig. 1 illustrates the model development framework.

The ISMM-PCI presented in this study is intended to assist the organizations and provided as a tool to evaluate and measure their information security capability (maturity) in order to proceed with the best strategies with the objective to achieve a full PCI DSS compliant, as well as meeting the objectives of security (confidentiality, integrity, and availability), while anticipating attacks, improving the security posture and achieving organizations mission.

The model utilizes controls defined in ISO/IEC 27002:2013 [7][8], that facilitates the measurement of the current state of the information security management by the use of maturity model and provides an assistance in taking the appropriate and achievable improvement actions, attributed to risks.

The model utilizes both quantitative and qualitative analysis to measure and determine the current state of the organization's information security (maturity). It allows the organizations to identify the source of weaknesses based on the level of position (departmental) as well as the key success factors affecting PCI DSS compliance. This will assist the organizations to focus on the filling-in the gaps and come up with an action plan according to the suggested results. The ISMM-PCI model with strategic options is shown in Table I.

TABLE I
ISMM-PCI MODEL WITH STRATEGIC OPTIONS

Elements	Maturity Level Dimension			
	0=None	1=Initial	2=Basic	3=Capable
Philosophy		Information Security is Necessary	Information Security Must be Integrated Into Organization	Information Security is Part of the Culture
People (PP)		Security Awareness	Security Awareness	Security Awareness
Process (PR)		Undocumented Processes	Formalized Information Protection Documented Policies, Standards & Procedures	Formalized Information Protection Documented Policies, Standards & Procedures
Technology (TC)		Basic Computer and Network Protection	Basic Computer and Network Protection Technologically Updated Security Management	Basic Computer and Network Protection Technologically Updated Security Management Governance of Enterprise IT
Strategic Options	**S-01**	**S-02**	**S-03**	**S-04**
Information Security Trends: 2005–2007, Gartner Group (Brynes, 2005).	Review Status Quo	Establish Security Team Develop New Policy Set Initiate Strategic Program Design Architecture	Institute Processes Conclude Catch-Up Projects	Track Technology and Business Change Continuous Process Improvement

The ISMM-PCI defines components used to manage, measure, and control every aspect of security. It relies on three core components (people, process, and technology), used to benchmark and assist organizations to better understand security requirements and needs to achieve the required compliance. The model allows the organizations to identify the key success factors as well as the source of weaknesses according to the roles and responsibilities (departmental position), affecting PCI DSS compliance. Additionally, the model is expected to assist the organizations to focus on the filling-in the gaps and come up with an action plan according to the suggested results based on their maturity levels.

PCI DSS compliance roadmap which defines the model coverage and the compliance assessments, shown in Fig. 2.

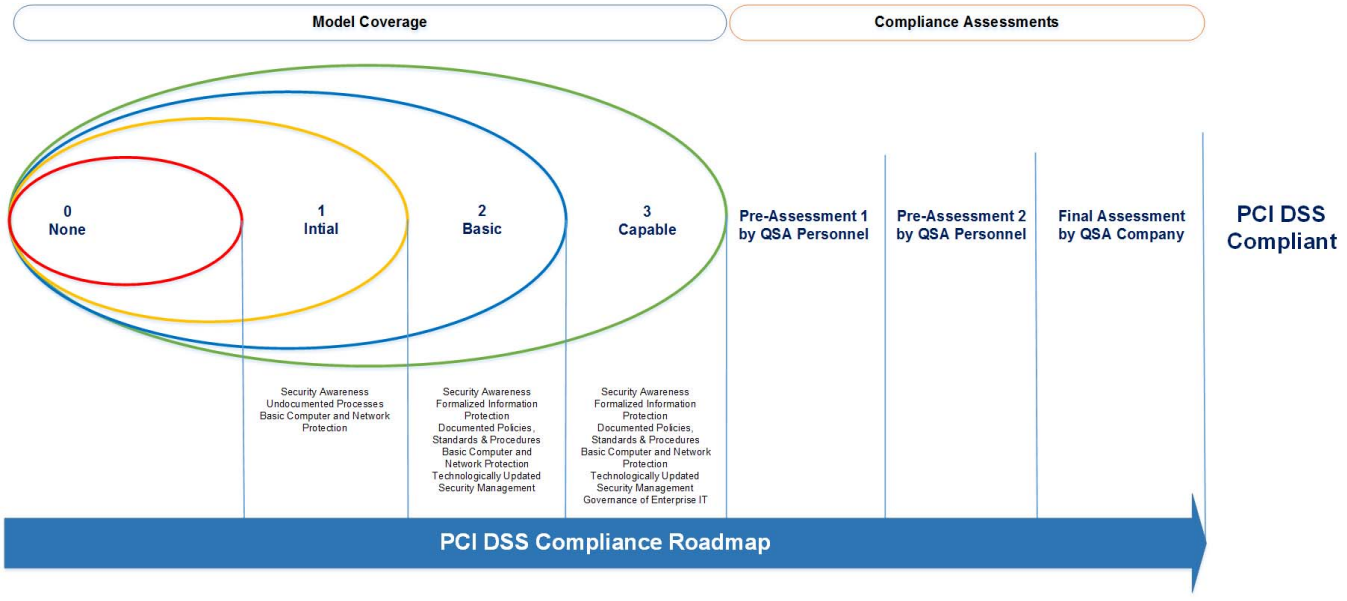

Fig. 2. PCI DSS Compliance Roadmap.

The roadmap allows the organizations to focus on enhancing the state of their information security while developing the action plan that will support the compliant achievement.

The ISMM-PCI model defines three core components to benchmark and assist organizations to better understand security requirements and needs to achieve compliance, they are Elements, Maturity Dimension and Strategic Options. Elements defined, represents the basic elements of information security in order to achieve the CIA (confidentiality, integrity and availability), which consist of People, Process and Technology. Three maturity levels defined in Maturity Level Dimension, they are 0 (None), 1 (Initial), 2 (Basic), 3 (Capable), used in measuring the initial maturity level of targeted organizations in order to satisfy the twelve high-level PCI DSS requirements. Strategic Options represent the best strategy that the organizations can focused on based on the determined maturity level (achievable). Options may include generic and/or specific actions adopted from the information security trends or industry best practices. These options could later be gathered as part of the information security strategic program and projected in the enterprise information security roadmap.

IV. Model Evaluation

This study takes advantages of the model evaluation based on comparative analysis of empirical data (collected data from the surveys), audit report (report on compliance), and the expert panel review. Despite advantages and disadvantages of each method, combination of several methods would contribute the most to the model in development. [1][20]

Comparing the results produced by the empirical data analysis with the actual real-life data collected from the audit reports – in this case Report on Compliance (ROC), is the next step in model evaluation. The expected results should show the significant of findings based on the compared information. At this stage, the accuracy of the model is tested against the live data as the output of the external factor evaluation conducted by a PCI DSS Qualified Security Assessor (QSA). Fig. 3 summarizes the model evaluation process.

Responses collected from the targeted organizations were then analyzed with the proposed methodology and model. Results were compared to determine the key success factors effecting the successful of PCI DSS compliance as well as the current state of the organizations information security maturity level. Table II shows the results comparison summary.

The selected methodology used in this study takes the advantages of the internal and external evaluation factors which influence a business. The internal evaluation factors, defined as the Internal Factor Evaluation (IFE), would normally represent the Strengths and Weaknesses, while the external evaluation factors, defined as the External Factor Evaluation (EFE) would normally represent the Opportunities and Threats to a business. The IFE utilizes Questionnaire (Q), while the EFE) utilizes Interview (I) and Direct Observation (D). Additionally, a simple formula representing the maturity level based on the weight of three core components (people, process, and technology) calculated against their secondary dataset (questionnaire).

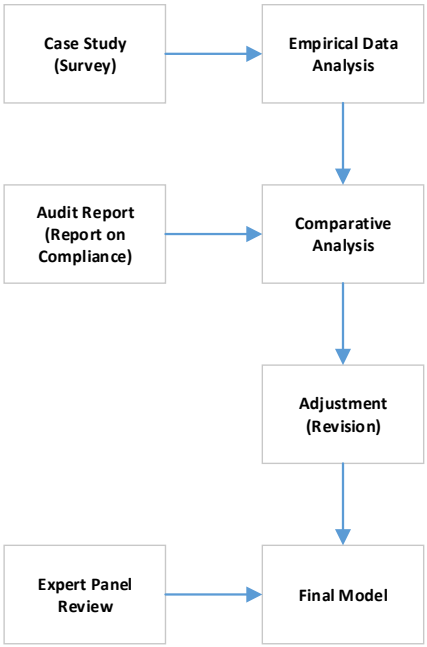

Fig. 3. Model Evaluation

TABLE II
RESULTS COMPARISON

Method of Analysis		Company A	Company B	Company C
Internal Factor Evaluation (IFE)	Questionnaire (Q)	19.22	25.22	04.67
External Factor Evaluation (EEF)	Interview (I)	10.71	15.00	06.41
	Direct Observation (D)	13.00	21.00	09.00
IEF + EEF = Q + I + D		**42.93**	**61.22**	**20.08**
ML = (WPP x Q1-PP) + (WPR x Q2-PR) + (WTC x Q3-TC)		**06.55**	**08.23**	**01.56**
Maturity Level (ML)		**1=Initial**	**2=Basic**	**0=None**
Key success factors of PCI DSS Compliance		People (30.06%)	People (35.68%)	People (33.33%)
		Process (27.17%)	Process (34.36%)	Process (33.33%)
		Technology (42.77%)	Technology (29.96%)	Technology (33.33%)
Contribution to the success of PCI DSS Compliance based on role and responsibility		Strategic (10.40%)	Strategic (23.79%)	Strategic (0.00%)
		Tactical (8.67%)	Tactical (12.78%)	Tactical (7.14%)
		Operational (80.92%)	Operational (63.44%)	Operational (92.86%)

The IFE & EFE results comparison of Company A (42.93), B (61.22) and C (20.08) suggested that Company B has achieved a higher Maturity Level (ML) compared to Company A and C. The resulting ML formula also suggested the same for Company B (8.23), compared to Company A (6.55) and C (1.56). In summary, both method of analysis presented by ISMM-PCI, affirms the organizations' information security capability in accordance to their respective maturity levels.

In addition to the information security maturity levels, the results also show that people and process were identified as the key success factors affecting PCI DSS compliance, while technology also supports the requirements but does not give a significant impact. Company B with maturity level Basic, put more efforts to people and process, while Company A with maturity level 1 (Initial), puts more efforts in technology enhancement. It looks like there is no significant efforts were given to people and process by Company C with maturity level 0 (None).

Contribution to the success of PCI DSS compliance based on role and responsibility, identified to be coming from the strategic level of users, followed by tactical, and operational. Strategic level of users (i.e. Managers) play an important role to a successful information security standards and frameworks adoption (top-down approach) as shown by Company A with maturity level 1 (Initial), and Company B with maturity level 2 (Basic). Company C with maturity level 0 (None), appears to have no support from the top management, since the operational level of users put more efforts for the same objectives (bottom-up approach).

V. Model Validation

Once the conceptual model was finalized, the accuracy and effectiveness of the model needs to be validated. The process of evaluating the model includes validation. Validation activities focuses on testing the accuracy of the model against the comparisons of experimental data or the actual real world situation which can be achieve by comparing the results taken from the actual reports with the data taken from the surveys. Information security experts and professionals play an important role in model validation, therefore the draft of the model is sent for the expert panel comments. Observations received shall be quantified, analyzed and summarized. Based on the feedbacks gathered from the experts' opinion, necessary adjustment or amendments will be made before the final research presentation.

In order to support and validate the effectiveness of model to be adopted and implemented by organizations, expert panel review was conducted. Individuals representing the industry experts with professional and academic qualifications, were selected based on certain criteria (panel members). The selected panel members consist of 5 (five) representative experts which were selected from the total of 7 (seven) respondents that responded to the request in participating the expert panel review, and have been filtered based on the criteria in order to satisfy the requirements. Responses in the form of feedbacks were then collected and analyzed.

The results of expert panel review are provided to affirm the validity of the proposed model. It is expected to support the statement regarding the effectiveness of the model in terms of adoption and implementation in heterogeneous organizations (e.g. financial institutions or any organizations within the same business line). The results of the expert panel review suggested that the proposed model helps the organizations to measure the maturity level of their information security (current state) to fully comply with PCI DSS (future state).

As recommended by the expert panel review, the ISMM-PCI should be enhanced not only by mapping PCI DSS with ISO 27001:2013 but also others relevant frameworks such as COBIT 5 for Information Security or BMIS (Business Model for Information Security). Recommendations include the use of ISO 15504 Process Assessment Standard (PAS) to leverage ISMM assessment attributes, indicators and dimensions. The measurement of people needs to be enriched, specifically related to the method on how to define maturity level and criteria of measurement. Additionally, it is recommended to design the mechanism in order to enable adjustment for the proposed model (e.g. ISMM continuum).

Furthermore, a comprehensive and in-depth security program should also consider many diverse areas of security, covering the management, operational, and technical security controls. This include (but not limited to), the overall policy, organizational structure, personnel related concerns or issues, and physical security. Non-technical aspects of information security should be supported by a baseline of information security measures and controls, as the new emerging types of attacks are rapidly grown and evolving. The 20 Critical Security Controls for Cyber Defense (CSC) provides structured and comprehensive baseline of crucial information security measures and controls which could be adapted and exercised across an organization, aim to improve its cyber defense.

The integration of ISMM-PCI with the CIS Critical Security Controls (CSC) would provide the organization with a proper readiness prior to maturity level assessment. It allows the organizations to tackle and reinforce the required practices for protecting against common threats to the business. The expected outcome is that both audit compliance and security objectives can be achieved. CSC would assist an organization to lively discover any weaknesses in IT infrastructure and security strategy concerning people, process, and technology. It allows the organization to quickly identify and tackle the emerging cyber-attacks, malicious activities, attack patterns, suspicious user behavior, vulnerabilities, and un-authorized access to system, while focusing on improving the overall information security.

VI. Conclusion

The proposed method in this paper is based on both quantitative and qualitative approaches that utilizes different data collection instruments to analyze and assess information security capability (maturity). The model consists of four maturity level - None, Initial, Basic and Capable. The proposed ISMM-PCI model is meant to be as a mechanism or tool to measure and determine the organizations' information security maturity. The model assists the organizations to easily identify the key success factors & gaps (point of weaknesses), provides the guideline to better manage information security and formulate the best strategy for the enhancement, with the goal to achieve full PCI DSS compliant, while improving the overall information security maturity. The main advantage of ISMM-PCI over other ISMMs is its ease of use. The comparative analysis of the case results affirms the statement. ISMM-PCI may be used by a wide range of organizations regardless of the size. Future work will include measuring the time, cost, and efforts given to PCI DSS implementation based on the model's

approach. It is also beneficial to include the most updated version of 20 Critical Security Controls for Effective Cyber Defense (CIS-CSC), COBIT 5 for Information Security or BMIS (Business Model for Information Security), and ISO 15504 Process Assessment Standard (PAS) to leverage ISMM assessment attributes indicators and dimensions [8].

ACKNOWLEDGMENT

The author would like to acknowledge the contribution of dedicated information security professionals and practitioners for their valuable efforts in developing the model. Validation would not be possible without their priceless involvement.

REFERENCES

[1] Alencar Rigon, E., Merkle Westphall, C., Ricardo dos Santos, D. and Becker Westphall, C., 2014. A cyclical evaluation model of information security maturity. Information Management & Computer Security, 22(3), pp.265-278.

[2] Cherdantseva, Y. and Hilton, J., 2013, September. A reference model of information assurance & security. In Availability, reliability and security (ares), 2013 eighth international conference on (pp. 546-555). IEEE.

[3] Coertze, J. and von Solms, R., 2012. A model for information security governance in developing countries. In e-Infrastructure and e-Services for Developing Countries (pp. 279-288). Springer Berlin Heidelberg.

[4] Dzazali, S., Sulaiman, A. and Zolait, A.H., 2009. Information security landscape and maturity level: Case study of Malaysian Public Service (MPS) organizations. Government Information Quarterly, 26(4), pp.584-593.

[5] Esteves, J. and Joseph, R.C., 2008. A comprehensive framework for the assessment of eGovernment projects. Government information quarterly, 25(1), pp.118-132.

[6] International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 2013, ISO/IEC 27001:2013, Information Security Management System (ISMS) - Requirements.

[7] International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 2013, ISO/IEC 27002:2013, Information Security Management System (ISMS) - Code of practice for information security controls.

[8] International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 2004, ISO/IEC 15504-1:2004 Information technology -- Process assessment -- Part 1: Concepts and vocabulary

[9] Karokola, G., Kowalski, S. and Yngström, L., 2011, August. Towards An Information Security Maturity Model for Secure e-Government Services: A Stakeholders View. In HAISA (pp. 58-73).

[10] Lee, G. and Kwak, Y.H., 2012. An open government maturity model for social media-based public engagement. Government Information Quarterly, 29(4), pp.492-503.

[11] Lessing, M.M., 2008. Best practices show the way to Information Security Maturity.

[12] Lovrić, Zrinka 2012, Model of Simplified Implementation of PCI DSS by Using ISO 27001 Standard. , pp.347–351.

[13] Matrane, O. & Talea, M., 2014. Towards A New Maturity Model for Information Security Management. , 4(6), pp.71–78.

[14] Payment Card Industry (PCI) 2013, Data Security Standard Requirements and Security Assessment Procedures.

[15] PCI 2013, Payment Card Industry (PCI) Data Security Standard, Version 3.0. Available at: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

[16] Ramanauskaitė, S. et al., 2014. Visualization of Mapped Security Standards for Analysis and Use Optimisation. , 6(5), pp.3–7.

[17] Ramanauskaitė, S., Olifer, D., Goranin, N. and Čenys, A., 2013. Security ontology for adaptive mapping of security standards. International Journal of Computers, Communications & Control (IJCCC), 8(6), pp.813-825.

[18] Saleh, M.F., 2011. Information Security Maturity Model. , (5), pp.316-337.

[19] Srivastav, A. et al., 2014. A Simple Prototype for Implementing PCI DSS by Using ISO 27001 Frameworks. , 4(1), pp.886–889.

[20] Thacker, B.H., Doebling, S.W., Hemez, F.M., Anderson, M.C., Pepin, J.E. and Rodriguez, E.A., 2004. Concepts of model verification and validation (No. LA-14167). Los Alamos National Lab., Los Alamos, NM (US).